Canada's Nuclear Regulator

Security:

Security of Nuclear Substances: Sealed Sources

REGDOC-2.12.3

May 2013

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Security of Nuclear Substances: Sealed Sources
Regulatory Document REGDOC-2.12.3

PWGSC catalogue number CC174-3/2-12-3E-PDF

ISBN 978-1-100-22178-6

Published by the Canadian Nuclear Safety Commission (CNSC)

Également publié en français sous le titre de : La sécurité des substances nucléaires : sources scellées

Document availability

This document can be viewed on the CNSC Web site at nuclearsafety.gc.ca or to request a copy of the document in English or French, please contact:

Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, Ontario K1P 5S9
CANADA

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Facsimile: 613-995-5086
Email: info@cnsc-ccsn.gc.ca
Web site: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn

Publishing history:

May 2013 Version 1.0

Preface

This regulatory document is part of the CNSC's Security series of regulatory documents, which also covers high-security facilities and site security. The full list of regulatory document series is included at the end of this document and can be found on the CNSC's Web site at nuclearsafety.gc.ca/regulatory-documents

Regulatory document REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources* sets out the minimum security measures that licensees must implement to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of sealed sources during their entire lifecycle, including while the sources are in storage, transport or being stored during transportation.

This document also provides information and guidance on how to meet the minimum security measures, including measures related to transport vehicles, containers and security plans. This document applies to transport by road within Canada only (there are other instruments and technical instructions that regulate the safe transport of dangerous goods by sea, air and rail).

Requirements associated with this document are found in the *Nuclear Safety and Control Act* (NSCA) and regulations made under it.

This document is intended to form part of the licensing basis for a regulated facility or activity. It is intended for inclusion in licences as either part of the conditions and safety and control measures in a licence, or as part of the safety and control measures to be described in a licence application and the documents needed to support that application.

In September 2003, the International Atomic Energy Agency (IAEA) approved the *Code of Conduct on the Safety and Security of Radioactive Sources*. Canada, along with many other countries, has undertaken to abide by this Code and work toward its full implementation. REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources* supports the regulatory framework to enforce international guidelines set by the IAEA, and provides consistency in the application of security measures.

The *Packaging and Transport of Nuclear Substances Regulations* (PTNSR) apply to consignors, consignees, and carriers. However, sub-contractors are not licensed by the Canadian Nuclear Safety Commission (CNSC) and, therefore, are not subject to the security requirements applicable to CNSC licensees. This regulatory document is intended to assist licensees with contracting carriers, so as to ensure that specific security measures are taken into consideration when transporting sealed sources, during storage, or storing them while in transit.

Security of Nuclear Substances: Sealed Sources, reflects the security goals of United Nations specialized agencies and programs – including the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO) and other intergovernmental organizations such as the International Carriage by Rail – as they have taken similar steps to provide improved security in the transport of dangerous goods carried by sea, air and rail. These organizations have developed various instruments, such as the *International Maritime Dangerous Goods Code,* and technical instructions for the safe transport of dangerous goods by air.

This document applies to sealed radioactive sources (encapsulated or solid) and does not apply to unsealed radioactive substances. This document applies to category 1, 2, and 3 sources and provides "prudent management practices" for category 4 and 5 sources. In this document, the terms category 1 to 5 sources are used as defined in the IAEA's *Code of Conduct on the Safety and Security of Radioactive*

Sources, IAEA Safety Guide RS-G-1.9, *Categorization of Radioactive Sources* or IAEA/TECDOC-1344, *Categorization of Radioactive Sources*.

Important note: Where referenced in a licence either directly or indirectly (such as through licensee-referenced documents), this document is part of the licensing basis for a regulated facility or activity.

The licensing basis sets the boundary conditions for acceptable performance at a regulated facility or activity and establishes the basis for the CNSC's compliance program for that regulated facility or activity.

Where this document is part of the licensing basis, the word "shall" is used to express a requirement to be satisfied by the licensee or licence applicant. "Should" is used to express guidance or that which is advised. "May" is used to express an option or that which is advised or permissible within the limits of this regulatory document. "Can" is used to express possibility or capability.

Nothing contained in this document is to be construed as relieving any licensee from any other pertinent requirements. It is the licensee's responsibility to identify and comply with all applicable regulations and licence conditions.

Table of Contents

Security of Nuclear Substances: Sealed Sources

1. Introduction

1.1 Purpose

Regulatory document REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources* sets out the minimum security measures that licensees must implement to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of sealed sources during their entire lifecycle, including while they are in storage, transport or being stored during transportation.

1.2 Scope

This document describes the minimum security measures required for the storage of sealed sources, and includes measures for both technical and administrative physical security. It includes measures related to transport vehicles, containers and security plans. This document also provides information and guidance on how to meet the security requirements.

The *Packaging and Transport of Nuclear Substances Regulations* (PTNSR) apply to consignors, consignees, and carriers (both licensees and non-licensees). *Security of Nuclear Substances: Sealed Sources* provides guidance to licensees to ensure that security measures are in place to protect radioactive material during transport. If third-party carriers are used to transport radioactive material, this regulatory document also sets out the minimum security measures that a licensee must ensure a carrier of sealed sources meets while the sealed sources are in transport or being stored during transportation.

This document applies to transport by road within Canada only (there are many instruments and technical instructions that regulate the safe transport of dangerous goods by sea, air and rail).

This document applies to sealed radioactive sources (encapsulated or solid) and does not apply to unsealed radioactive substances. This document applies to category 1, 2, and 3 sources and provides "prudent management practices" for category 4 and 5 sources. In this document, the terms category 1 to 5 sources are used as defined in the International Atomic Energy Agency's (IAEA) *Code of Conduct on the Safety and Security of Radioactive Sources* [1], IAEA Safety Guide RS-G-1.9, *Categorization of Radioactive Sources* [2] or IAEA/TECDOC-1344, *Categorization of Radioactive Sources* [3] (see also glossary).

1.3 Relevant legislation and regulations

The following provisions of the *Nuclear Safety and Control Act* (NSCA) and regulations made under the NSCA are relevant to this regulatory document:

- paragraphs 3(1)(*g*) and (*h*) of the *General Nuclear Safety and Control Regulations* state that "an application for a licence shall contain the following information: […]
  (*g*) the proposed measures to control access to the site of the activity to be licensed and the nuclear substance, prescribed equipment or prescribed information;
  (*h*) the proposed measures to prevent loss or illegal use, possession or removal of the nuclear substance, prescribed equipment or prescribed information"
- paragraphs 12(1)(*c*), (*g*), (*h*) and (*j*) of the *General Nuclear Safety and Control Regulations* state that "every licensee shall […]

(*c*) take all reasonable precautions to protect the environment and the health and safety of persons and to maintain the security of nuclear facilities and of nuclear substances; […]
(*g*) implement measures for alerting the licensee to the illegal use or removal of a nuclear substance, prescribed equipment or prescribed information, or the illegal use of a nuclear facility;
(*h*) implement measures for alerting the licensee to acts of sabotage or attempted sabotage anywhere at the site of the licensed activity; […]
(*j*) instruct the workers on the physical security program at the site of the licensed activity and on their obligations under that program"

- sections 21, 22, and 23 of the *General Nuclear Safety and Control Regulations* define prescribed information and provide details on which persons may possess, transfer, import, export, use, or disclose prescribed information
- subsection 28(1) of the *General Nuclear Safety and Control Regulations* states that "every person who is required to keep a record by [the NSCA], the regulations made under [the NSCA] or a licence shall retain the record for the period specified in the applicable regulations made under [the NSCA] or, if no period is specified in the regulations, for the period ending one year after the expiry of the licence that authorizes the activity in respect of which the records are kept"
- paragraphs 36(1)(*a*) and (*d*) and subsection 36(2) of the *Nuclear Substances and Radiation Devices Regulations* state that:
  "(1) Every licensee shall keep the following records:
  (*a*) a record of the following information in respect of any nuclear substance in the licensee's possession that is referred to in the licence:
  (i) the name, quantity, form and location of the nuclear substance,
  (ii) where the nuclear substance is a sealed source, the model and serial number of the source,
  (iii) where the nuclear substance is contained in a radiation device, the model and serial number of the device,
  (iv) the quantity of the nuclear substance used, and
  (v) the manner in which the nuclear substance was used;
  …
  (*d*) a record of the training received by each worker
  …
  (2) Every licensee shall retain a record referred to in paragraph (1)(*d*) for the period ending three years after the termination of employment of the worker"
- section 17 of the *Packaging and Transport of Nuclear Substances Regulations* states that "every consignor of radioactive material shall include in the transport documents for the consignment the information referred to in paragraph 549 of the *IAEA Regulations* [4] which shall be clearly and indelibly printed in the documents"

The *Transportation of Dangerous Goods Regulations* (Transport Canada) may also apply to sealed sources.

1.4 National and international standards

This regulatory document is consistent with modern national and international guides and standards for physical security measures for sealed sources. Publications relevant to physical security of sealed sources include:

- IAEA, *Code of Conduct on the Safety and Security of Radioactive Sources*, 2004 [1]
- IAEA Safety Guide RS-G-1.9, *Categorization of Radioactive Sources* [2]
- IAEA, TECDOC-1344, *Categorization of Radioactive Sources*, 2003 [3] (Revision of IAEA-TECDOC-1191, *Categorization of Radiation Sources*, 2000)
- IAEA, TS-R-1, *Regulations for the Safe Transport of Radioactive Material*, 1996 edition (revised) [4]
- IAEA, TECDOC-1355, *Security of Radioactive Sources – Interim Guidance for Comment*, 2003 [5]
- IAEA, TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities*, 2002
- IAEA, *Security in the Transport of Radioactive Material*, 2008
- IAEA, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*, 2011

2. Background

Radioactive sealed sources and prescribed equipment containing nuclear substances are regulated under the *Nuclear Safety and Control Act* (NSCA) and the regulations made under the NSCA, such as the *General Nuclear Safety and Control Regulations*, *Class II Nuclear Facilities and Prescribed Equipment Regulation*, *Nuclear Substances and Radiation Devices Regulations* and the *Radiation Protection Regulations*.

Additional regulations related to the transport of sources (such as packaging, documentation and safety markings) include:

- Canadian Nuclear Safety Commission (CNSC), *Packaging and Transport of Nuclear Substances Regulations* (PTNSR)
- Transport Canada, *Transportation of Dangerous Goods Regulations*

This document uses a graded approach for the security of sealed sources. There are five levels of sealed sources (categories 1 through 5). This document provides requirements that apply to radioactive sealed sources that may pose a significant risk to the environment and the health and safety of persons (i.e., category 1, 2 and 3 sources). Because categories 4 and 5 are the least dangerous sealed sources, this document provides prudent management practices for those categories.

2.1 Application

This regulatory document applies to sealed sources of nuclear substances identified in table A. These substances and threshold values are based on the IAEA *Code of Conduct on the Safety and Security of Radioactive Sources* [1]. The main objective of this regulatory document is specific to radioactive sources that could be dangerous to the health and safety of persons and to the environment if they are not protected.

As outlined in IAEA TECDOC-1344 [3], if a practice involves the accumulation of several sources into a single storage or use location, where these sources are in close proximity or collocated (such as in storage facilities, manufacturing processes, or transport conveyance), the total activity is treated as a single source for the purpose of assigning a category. When sources are stored or used in separate controlled locations, they may have independent security measures commensurate with the activity level of the source; in this case, aggregation considerations are not applicable. In some circumstances, an entire site is not considered a single controlled use or storage location.

The security requirements must be commensurate with the categorization, threat level and/or level of risk set by the licensee or the Government of Canada. Note that mobile and portable radioactive sources may need to be treated differently, to ensure that any specific security requirements are fulfilled, thereby allowing the source to be used as intended.

2.2 Categorization of sources

The CNSC bases its categorization of sources on the IAEA source categorization, defined in IAEA TECDOC-1344 [3]. This document recognizes that not all radioactive sources could (or should) be treated alike, and has established five source categories, ranging from category 1 (extremely dangerous) to category 5 (unlikely to be dangerous). The IAEA categorization methodology has found worldwide acceptance, and provides a uniform means of classifying the risk associated with the most commonly used radioactive sealed sources and radiation devices.

Sealed sources and radiation devices may be used in one location (for example, fixed gauges used on process equipment), or they may be mobile and used on different job sites (for example, radiography exposure devices and portable soil moisture density gauges).

Category 1 sources are the most dangerous sealed sources licensed by the CNSC. Because they pose the greatest risk to the health and safety of persons and to the environment, category 1 sources are always used in a well-shielded and well-controlled location. Examples include cobalt-60 teletherapy sources used for cancer treatment and cobalt-60 sources used in pool-type irradiators to sterilize medical products. Such sources must be shielded and secured safely.

The most common example of a category 2 source is an industrial radiography exposure device. These devices are portable, and are widely used in pipeline work and in pressure vessel fabrication shops (particularly in the oil and gas industry).

Category 3 sources are often fixed gauges that are bolted to pipes, vessels and assembly lines where they operate reliably in harsh industrial environments, often for decades.

Category 4 sources are less dangerous than category 3 sources, and are classified as low risk to persons, security and the environment. An example of a category 4 source is a portable soil moisture density gauge used in road construction.

Category 5 sources and their use are considered to be the least dangerous. Examples include electron capture detectors used to measure pesticide residues in food, x-ray fluorescence analyzers, and low-dose brachytherapy implant sources. Some category 5 sources may be used without a CNSC licence.

Table A provides thresholds of category 1, 2 and 3 sources, measured in activity level. Appendix C provides examples of category 1, 2 and 3 sources by “use type”.

Table A: Activities corresponding to thresholds of category 1, 2 and 3 sources

Radionuclide	Category 1 source		Category 2 source		Category 3 source	
	Terabecquerels (TBq)	Curies (Ci)	Terabecquerels (TBq)	Curies (Ci)	Terabecquerels (TBq)	Curies (Ci)
Americium-241 (^{241}Am)	60	1,600	0.6	16	0.06	1.6
Americium-241 / Beryllium (^{241}Am/Be)	60	1,600	0.6	16	0.06	1.6
Californium-252 (^{252}Cf)	20	540	0.2	5	0.02	0.5
Cesium-137 (^{137}Cs)	100	2,700	1	27	0.1	2.7
Cobalt-60 (^{60}Co)	30	810	0.3	8	0.03	0.8
Curium-244 (^{244}Cm)	50	1,350	0.5	13	0.05	1.3
Gadolinium-153 (^{153}Gd)	1,000	27,000	10	270	1	27
Iridium-192 (^{192}Ir)	80	2,160	0.8	21	0.08	2.1
Plutonium-238 (^{238}Pu)	60	1,620	0.6	16	0.06	1.6
Plutonium-239 / Beryllium (^{239}Pu/Be)	60	1,620	0.6	16	0.06	1.6
Promethium-147 (^{147}Pm)	40,000	1,080,000	400	10,080	40	1,100
Radium-226 (^{226}Ra)	40	1,080	0.4	11	0.04	1.1
Selenium-75 (^{75}Se)	200	5,400	2	54	0.2	5.4
Strontium-90 (^{90}Sr) / (Yttrium-90 (^{90}Y)	1,000	27,000	10	270	1	27
Thulium-170 (^{170}Tm)	20,000	540,000	200	5,400	20	540
Ytterbium-169 (^{169}Yb)	300	8,100	3	81	0.3	8.1

Thresholds for the activity levels

The materials and thresholds in Table A are based on the IAEA *Code of Conduct on the Safety and Security of Radioactive Sources* [1]. These thresholds aim to provide consistency between domestic and international requirements for the protection of radioactive material.

The IAEA *Code of Conduct on the Safety and Security of Radioactive Sources* [1] lists 16 radionuclides that could pose a serious threat to the health and safety of people and to the environment. Irradiated fuel and mixed oxide fuel are not included in the list even though they contain quantities of radioactive material; these materials are covered by the *Nuclear Security Regulations*.

The terabecquerel (TBq) is the official measurement unit used for determining whether a radioactive material is a category 1, 2, or 3 source. Because many licensees use Curies in their activities instead of Becquerels, the table also provides the equivalent Curie (Ci) measurement, for practical usefulness.

IAEA RS-G-1.9, *Categorization of Radioactive Sources* [2] provides the methodology for the development of the *Code of Conduct* thresholds.

These regulatory requirements apply only to sealed sources. However, it is recommended that comparable security requirements be taken into account for open or unsealed sources when considering the suitability and adequacy of the storage arrangements.

Methodology for assigning a category

To assign a category, the total activity of all sources in one facility (storage or use) where sources are in close proximity must be equal to, or greater than, the number identified in the category. For example:

- a teletherapy medical device with a sealed source up to 555 TBq of cobalt-60 is a category 1 source (555 > 30)
- a certified radiography exposure device with a sealed source of 2.5 TBq of iridium-192 is a category 2 sealed source (80 > 2.5 > 0.8)
- a high dose rate (HDR) brachytherapy medical device with a sealed source up to 0.44 TBq of iridium-192 is a category 3 source (0.8 > 0.44 > 0.08)

For security control purposes, the aggregation of sources in a single storage (or use) facility can be used to determine a situation-specific sealed source category. This is done by adding the actual sealed source activities of the sources and determining the category from Table A. For example, one industrial level gauge containing a sealed source with 0.19 TBq of cesium-137 is a category 3 source (1.0 > 0.19 > 0.1). However, when there are six of these sealed sources at a single licensed location, for security reasons they may be treated as a category 2 source (6 x 0.19 = 1.1 > 1.0).

The A/D ratio for a single radionuclide is the activity (A) of the source compared to the activity determined to define a threshold of danger (D). For the aggregation of various radionuclides, the sum of the A/D ratios is used to determine a final category as described in RS-G-1.9, *Categorization of Radioactive Sources* [2] and TECDOC-1344, *Categorization of Radioactive Sources* [3]. If multiple sources from different categories are stored, the highest category should

suffice (e.g., storage of category 2, 3 and 4 sources would meet the security requirements for category 2).

3. Security Measures

3.1 General security measures

While in storage, licensees shall develop and implement technical and administrative security measures to protect the radioactive source against unauthorized removal (such as theft or loss) or sabotage.

As outlined in IAEA TECDOC-1355 [5], these measures shall integrate safety and security concepts involving industrial safety arrangements, radiation protection measures and appropriate design to achieve the necessary level of protection against unauthorized removal of radioactive sources.

Guidance

The security program should include security measures relating to detection, delay and response to security events (e.g., alarm detection devices, fencing, secured storage containers, immobilization of vehicles and/or trailers, and security officers).

The licensee should develop and maintain a threat and risk assessment to determine vulnerabilities in the existing physical protection systems designed to protect against the loss, sabotage, illegal use, illegal possession, or illegal removal during the storage or transportation of sealed sources. This could include:

- identification of assets that require protection
- credible threats
- mitigation measures to minimize any identified threats, risks or vulnerabilities

The threat and risk assessment should be reviewed annually and updated as required based on changes that affect the threat level.

The degree of rigor of a threat and risk assessment should follow the graded approach and should be commensurate with the category and risks associated with the sealed sources. This threat and risk assessment may be incorporated into existing assessments.

Table B provides information on how security program subsections should be applied to category 1 (high risk), category 2 (high risk), category 3 (medium risk), and categories 4 and 5 (low risk).

Table B: Security levels and security objectives

Security program sub sections	Category 1 - high risk	Category 2 - high risk	Category 3 - medium risk	Category 4 and 5 - low risk
Access control	• restrict access to authorized user only • two-person rule (optimal) • visitors, students, contractors must be escorted at all times by an authorized user	• restrict access to authorized user only • visitors, students, contractors must be escorted at all times by an authorized user	• restrict access to authorized user only • visitors, students, contractors must be escorted by an authorized user	• source should be protected against unauthorized access and removal
Intrusion detection system	• must provide immediate detection and be linked to a ULC-certified control room monitored by an operator 24/7 or an equivalent mechanism (i.e., continuous surveillance by operator) for detection, assessment, and communication with response personnel in case of security event			
Perimeter and/or physical barrier	• must be protected with at least two physical barriers (i.e., walls, cages, secure containers) to separate the source from unauthorized personnel and provide sufficient delay to allow for immediate detection, and for response personnel to intervene before the adversary can remove the source			
Security of storage	• secured with high quality padlock, high security lock or equivalent security system • equipped with a minimum of one intrusion detection system or equivalent • secure containers must be able to resist an attack by handheld tools		• secured with high quality padlock, high security lock or equivalent security system • equipped with a minimum of one intrusion detection system or equivalent	• should be stored in a secure container or location
Response protocol	• specific response protocol and contingency plan • contact local law enforcement • effective response time • must develop a procedure in case of lost, stolen or malicious act involving radioactive sealed source		• generic response protocol and contingency plan • must develop a procedure in case of lost, stolen or malicious act involving radioactive sealed source	• source should be protected against unauthorized access and removal
Maintenance and testing	• maintenance and testing must be conducted at least every six months, and written records should be maintained			

Security program sub sections	Category 1 - high risk	Category 2 - high risk	Category 3 - medium risk	Category 4 and 5 - low risk
Facility security plan	• reviewed annually or when important changes are done at the facility • classified prescribed and/or sensitive and stored appropriately • communicated on a need to know basis • indicate measures in case of increased threat		• reviewed on a regular basis or when important changes are done at the facility • must be classified prescribed and/or sensitive and stored appropriately • communicated on a need to know basis	• prudent management practice
Personal trustworthiness or background checks	• criminal records name check • reference, education and employment verification • drivers and contractors (i.e., carriers) with unescorted access to radioactive sources must undergo this verification		• reference, education and employment verification • criminal records name check	• reference, education and employment verification • criminal records name check (prudent management practice)
Information security	• all prescribed information must be protected and be shared on a need to know basis			
Security awareness program	• all authorized users, including staff who transport radioactive sources, must receive security awareness training on a regular basis			
Vehicle security	• vehicle must be equipped with anti-theft or vehicle disabler and intrusion detection system, or equivalent measures • vehicle must be equipped with a minimum of two technical barriers to prevent unauthorized removal of the radioactive source/device • access must be restricted to authorized users only • GPS or tracking system • drivers must be equipped with a means of communication in case of emergency • two-person rule (optimal) • drivers and operators must undergo a trustworthiness verification		• vehicle must be equipped with anti-theft and intrusion detection system or equivalent measures • vehicle must be equipped with a minimum of two technical barriers to prevent unauthorized removal	• source should be protected against unauthorized access and removal
Transportation security plan	• must develop and submit a specific Transport Security Plan to CNSC for review and approval	• must develop and maintain a generic Transport Security Plan	• prudent management practices	• source should be protected against unauthorized access and removal

3.2 Technical security measures

Technical security measures for radioactive sources, devices or facilities shall include physical measures to:

- prevent unauthorized personnel from gaining access to such sources
- protect against an act or attempted act of unauthorized removal
- protect against an act or attempted act of sabotage

Technical security measures shall also include hardware and/or security systems designed according to the principle of defence in depth and the physical protection system functions of "detection, delay and response".

This section includes security requirements for the following measures:

- access control
- detection of unauthorized access
- locking hardware and key control
- physical barriers (secure containers, secure enclosures)
- alarm response protocols
- inspection, maintenance and testing of physical security-related equipment
- security officers

Within each of the areas identified above, the licensee shall define appropriate security measures that are commensurate with the level of risk presented by the sealed source(s). Further details are provided in sections 3.2.2 to 3.2.8.

Pursuant to paragraphs 3(1)(*g*) and 3(1)(*h*) of the *General Nuclear Safety and Control Regulations*, the licensee shall include in their licence application details pertaining to physical security measures for access control, physical barriers, detection of unauthorized access, maintenance and testing of physical security-related equipment.

3.2.1 Access control

The licensee shall implement access control measures (e.g., access card readers, personnel identification systems, manual or electronic locks) or use security officers to ensure that only authorized persons have access to storage areas containing sealed sources at all times.

Visitors, building maintenance staff, servicing companies, students and contractors who require access to the sealed source storage shall be escorted at all times if they do not possess a trustworthiness verification approved by the licensee.

Guidance

To control access to the sealed sources, the licensee should consider the following measures, based on a graded approach:

- monitor and maintain records of all personnel with access to secure storage areas, through the use of a log book or an access control system with tracking capabilities
- implement effective access control measures such as manually activated locking devices, padlocks, card reader access, biometric devices/systems, and "controlled" entry points
- ensure the access control system incorporates measures to prevent unacceptable practices such as "pass back" or "tailgating"

- assign individual personal identification number (PIN) codes if used in conjunction with an access control system
- remove access rights for individuals as soon as access is no longer required
- restrict access rights to the access control management system and software, to prevent unauthorized interference with the system database (hacking, software sabotage)
- implement a means of duress signalling near the source storage, to provide notice to the alarm monitoring company or response personnel
- implement a local alarm that triggers in the vicinity of the storage area, to alert nearby personnel of an intrusion or other problem in the source storage area

The concept of escorting an individual at all times means maintaining line of sight with this individual.

3.2.2 Detection of unauthorized access

The licensee shall implement measures for the detection of attempted or actual unauthorized access in a timely manner, such as:

- visual observation
- video alarm assessment
- detection devices
- accountancy records, seals, or other tamper-indicating devices including process monitoring systems

Note that, for mobile sources in use, continuous visual surveillance by operator personnel equipped with an appropriate communication link may substitute for one or both layers of barriers.

If an intrusion detection system is used, it must:

- immediately detect any unauthorized intrusion into the sealed source storage area
- immediately detect any tampering that may cause any of the alarm system devices to malfunction or cease to function
- when an intrusion is detected, set off a continuous alarm signal that is both audible and visible at the licensee's location and/or at an approved monitoring station, using a supervised communications link
- include an uninterruptible power supply, subject to routine testing, to ensure continuous operability of the security detection system

Guidance

To detect unauthorized access, failure or tampering, the alarm system should:

- activate immediately upon detecting an intrusion or tamper event
- stay in an alarmed state until acknowledged by an authorized person
- use more than one sensor or sensor type in order to provide redundancy
- include overlapping sensor detection areas
- use dedicated supervised communication links that are continually monitored
- have dedicated alarm zones for each area of storage
- have a low nuisance and false alarm rate with a high probability of detection

For licensees who contract their alarm monitoring to third-party companies, the licensee should ensure that the monitoring company is certified by the Underwriters Laboratories (UL) or

Underwriters Laboratories of Canada (ULC), or other certification body deemed acceptable by CNSC staff.

In addition, the licensee should:
- ensure that alarm monitoring devices and back-up battery power are protected against tampering by unauthorized personnel (e.g., electronic panel or junction box)
- ensure the keypad is installed within a secure environment, to prevent tampering
- use dedicated alarm zones in the storage area (separate from any other alarm zones) and limit access to authorized users only
- maintain an audit trail to record the cause of any alarms
- ensure the alarm monitoring station is continuously staffed

For example, consider a radiography company that has a warehouse equipped with an alarm system. Two zones are set up: one zone for the warehouse and a second interior zone for the storage area. During the day, the main alarm system for the warehouse is deactivated but the security system for the storage area remains activated and operates independently of the main system.

3.2.3 Locking hardware and key control

Access cards, door keys, or locks that control access to storage areas shall be restricted to personnel authorized by the licensee.

The licensee shall maintain records of all access control authorizations, including locking devices (either electronic or manual). Such records shall include the names of the individuals to whom the locking devices or combinations have been issued, and the date of issuance.

The licensee shall develop and maintain written procedures that include measures for issuing, repairing or replacing a locking device, key, access card or combination that is defective, lost, stolen, or unlawfully transferred, or has otherwise become compromised.

Guidance

If keys are used, the licensee should implement a key control policy to:
- restrict the number of individuals with keys
- restrict the number of master keys
- prohibit employees from duplicating keys
- use a patented key or dedicated keyway to prevent unauthorized duplication of keys
- include a provision for employees to return keys when access is no longer required
- ensure that key blanks are stored securely

For key control, the licensee should:
- conduct a review of the key inventory and keyholders on a regular basis
- note changes and additions to the key inventory and keyholders in their records
- maintain accountability for all keys that have been issued and keys reported lost or stolen

Locks with combination codes or cipher-based keyless locks are not recommended.

When conventional locks and keys are used, they should be of high quality or from a high-security lock series. Key management procedures should be designed to prevent unauthorized access or compromise. The locks should have shielded shackles, to prevent cutting of the lock.

3.2.4 Physical barriers

For sealed sources whose activity is less than the threshold levels listed for category 3 in Table A, the licensee shall store the sources in secure containers, as described in section 3.2.5.1.1.

For sealed sources whose activity is equal to or above the threshold levels listed for categories 1, 2, or 3 in Table A, the licensee shall implement a minimum of two different physical barriers, to prevent unauthorized access to sealed sources in storage and provide delay sufficient to enable response personnel to intervene as required.

The physical barriers shall be any combination of secure containers or other secure enclosures. For example:

- a licensee who stores a sealed source in a locked safe may locate the safe in an enclosed room that can be locked, and must secure the container in place (floor, wall or vehicle)
- alternatively, the safe may be located within a locked metal cage or other suitable enclosure
- the access-controlled perimeter of the licensee's location may serve as the first secure enclosure, with a secondary secure enclosure or secure container inside, both with access control

Note that for a mobile source in use, it may not always be possible to achieve the security measures specified above. In such cases, compensatory measures shall be implemented to provide other forms of protection (e.g., close supervision combined with an appropriate communication link).

Note that sealed sources stored in pools may have safety features inherent to their design that may substitute for one or both layers of physical barriers.

Secure containers

Secure containers include items such as secure filing cabinets, metal boxes, safes, vaults and wire mesh cages. For a container to be considered secure, it must be:

- securely affixed in place
- resistant to physical attack using handheld tools
- fitted with a key or combination padlock, or similar lock, that can resist surreptitious or forced attack using handheld tools
- when a wire mesh cage is used, the cage fabric must be expandable metal mesh no smaller than number 10 gauge [6]

Note that sealed sources stored inside containers weighing over 500 kg may be considered secure due to their weight and robustness. Equivalent containers or structures that have a comparable level of security may be acceptable.

Secure enclosures

Enclosures include rooms, buildings or cages that can be secured. For an enclosure to be considered secure, all exterior components (e.g., walls, doors and windows) are resistant to physical attack using handheld tools and access/egress points are equipped with access control devices, or access is controlled by security officers.

Windows that provide access to interior areas in proximity to sources must be equipped with bars (where the gap between the bars must be less than 15 cm), metal grill, expanded metal mesh, and/or retrofitted with a UL/ULC certified security film or glazing. Security hardware attached to

windows must be affixed from the inside to prevent tampering, or fitted with tamper-resistant devices if fitted from the outside.

Doors that provide access to areas where radioactive sources are used, processed or stored must be secured when left unattended. Doors must be solid-core wood or metal clad and installed in a reinforced frame of equivalent material. Doors must be maintained in good state of repair and fitted with non-removable pinned hinges, if the hinges are mounted on the outside. Any door glazing or large vents (grills) must be fitted with security glazing or bars, metal grills, or equivalent. Grills must be secured in place with tamper-resistant devices.

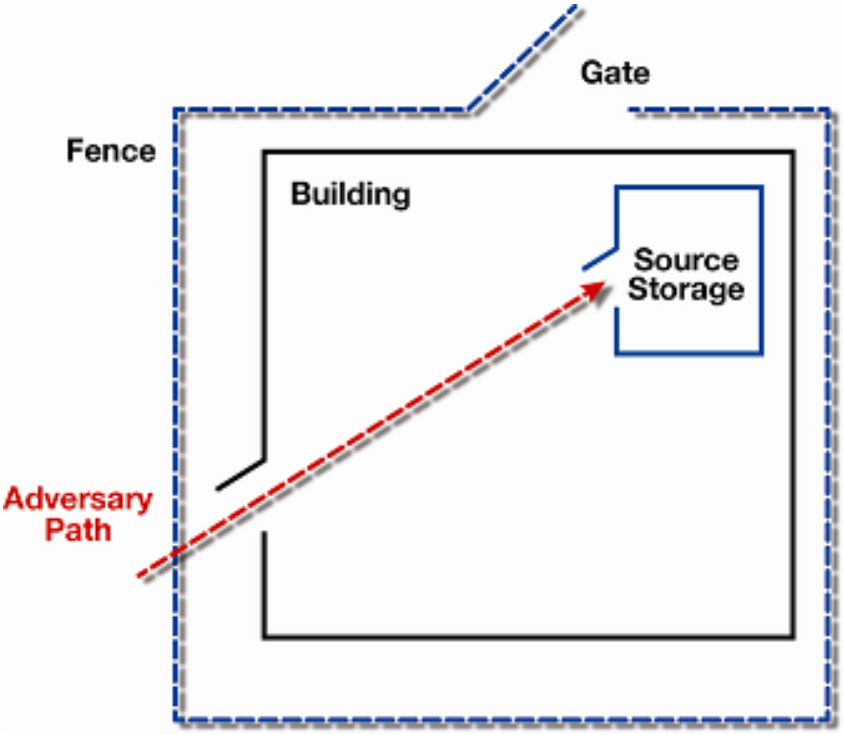
For situations where radioactive sources are used or stored in proximity to explosives, a minimum separation of 3 metres must be maintained between the radioactive sources and all explosive material, as required in section 13 of the *Guidelines for Jet Perforating Gun Assembly Facilities* [7].

Guidance

Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls and vaults are commonly used for storage of radioactive sealed sources. Barriers should be considered in relation to an adversary's objectives.

The licensee should implement multiple physical barriers to protect the radioactive sources. Multiple barriers potentially force an adversary to bring a variety of tools to defeat each individual barrier, thereby delaying the adversary and providing the response personnel with time to intervene. One implementation of the concept of defence in depth is to have multiple layers of different barrier types along the path to complicate an adversary's progress by requiring a variety of tools and skills (see figure 1).

Figure 1: Adversary path to a storage area



For example, multiple barriers may include:

- a portable device (e.g., portable gauge, exposure device) stored inside a vault or safe that is bolted to the floor and capable of resisting common attack tools
- a mobile device (e.g., a brachytherapy unit) may be chained to the floor within the storage area. The chain is made of material resistant to common attack tools and is secured with a high-quality padlock that has the same level of robustness (e.g., shielded shackles)
- a solid-core door made of wood or metal, installed with non-removable screws, pinned door hinges, a latch protector and an automatic door closer
- a window equipped with laminated window-film resistant to burglar attacks, metal mesh or metal bars spaced at 15 centimetres or less, and installed with non-removable screws

Guidance for secure containers

The storage location and/or container should:

- be secured with a locking mechanism or have other measures to prevent unauthorized removal
- be secured when left unattended
- be equipped with an alarm system to detect unauthorized entry or access
- be sufficiently robust to resist common attack tools (e.g., crowbar, drill, blowtorch)

Guidance for secure enclosures

Openings, such as windows or vent ducts, that could provide access to secure enclosures should be fitted with bars, a metal grill, expanded metal mesh, and/or retrofitted with a UL/ULC certified security film or glazing. Security hardware attached to windows should be affixed from the inside, to prevent tampering, or be fitted with tamper-resistant anchors if affixed from the outside.

Doors that provide access to areas where radioactive sealed sources and/or radiation devices are used, processed or stored should be secured when unattended. The material used for the door should be solid-core wood or metal-clad, and the door should be installed in a reinforced frame of equivalent material. Doors should be in a good state of repair. If the hinges are mounted on the non-secure side, the door should be fitted with non-removable pinned hinges. Any door glazing or large vents (grills) should be fitted with security glazing or bars, a metal grill, or equivalent. Grills should be secured in place with tamper-resistant anchors.

If continuous visual surveillance is done by an operator, the operator should be equipped with a means of communication (e.g., cell phone or radio) and should be aware of the response protocols to communicate rapidly to response personnel in the event of unauthorized access or removal.

If key pads are used to arm and disarm an intrusion detection system, the device and its electric junction box should be installed in a secure area, to reduce the risk of tampering.

To maintain continuous power to the alarm monitoring detection system in the event of a loss of primary power, the licensee should consider implementing an alternate or auxiliary power back-up source, or equivalent, to maintain detection capability.

3.2.5 Alarm response protocol

The licensee shall respond immediately to any actual or attempted theft, diversion or sabotage to radioactive material or devices.

The licensee shall develop and maintain a documented alarm response protocol to record the cause and dispensation of alarms. The protocol shall include the role and responsibilities of the licensee's emergency response staff and offsite response force, and shall be documented in a contingency plan or an equivalent document.

The licensee must notify the local law enforcement agency, informing them that sealed sources are onsite, and include an opportunity for onsite familiarization tours. The licensee shall develop and maintain written arrangements with offsite emergency responders, and update those arrangements annually or when changes to the facility design or operations affect the potential vulnerability of the source. Written arrangements are not required for temporary job sites.

Guidance

The licensee should develop and maintain a documented alarm response protocol that includes:
- response procedures in case of theft, loss or sabotage of a radioactive sealed source
- the role and responsibilities of the licensee's staff
- communication arrangements with local law enforcement and applicable authorities
- incident reporting/notification
- immediate reporting of any recovered source(s)

To facilitate arrangements with local or provincial law enforcement agencies, or mutual aid agreements with other sites, the licensee should consider written support arrangements such as a memorandum of understanding (MOU). This written arrangement should detail the interaction between site guards or onsite personnel with the agencies.

3.2.6 Inspection, maintenance and testing of security-related equipment

The licensee shall develop and implement written procedures for the testing of physical security equipment and a schedule for routine testing and maintenance in accordance with the manufacturer's specifications. At a minimum, testing of security equipment including intrusion detection devices shall be conducted every six months. The licensee shall demonstrate that alarm testing was conducted. Preventive maintenance procedures shall include measures to replace defective equipment and devices in a timely manner.

Guidance

All detection devices should be installed, operated and maintained in accordance with the manufacturers' specifications and licensee processes. The licensee should test the performance of the detection devices on a regular basis, to ensure reliability and maintain documented records.

Licensees should ensure reliability through a preventive maintenance program that tracks detection device deficiencies. When the device is out of service for repair or replacement, compensatory measures must be implemented.

3.2.7 Security officers

If the licensee uses a security guard service, the licensee shall develop and maintain written procedures and instructions specific to:
- measures for controlling access to the licensed area
- surveillance foot and vehicle patrols
- assessment and response to alarms
- apprehension and detainment of unarmed intruders
- report suspicious activities, including armed intruders, to the local law enforcement agency

- security equipment operation
- security training relating to assigned duties

Guidance

Security officers should be properly equipped and trained. A formal training program should be established that is specific to the security officers. The training program should include:

- requirements of provincial/territorial regulations (if applicable)
- legislation and authorities
- knowledge of the site
- roles, responsibilities and functions
- radiation protection emergency procedures and response protocols
- first-aid training techniques

Security officers should be screened in accordance with the trustworthiness program (see section 3.3.3) and should possess a valid licence or certification recognized by the province or territory.

The licensee should consider performing exercises and drills on a regular basis, to validate onsite response force readiness.

For security officers, the licensee should establish and maintain an overall training policy and initial and continuing training programs, based on the long-term qualifications and competencies required for performing the job, and training goals that acknowledge the critical roles of safety and security.

3.3 Administrative security measures

Administrative security measures support technical measures, and shall include the programs, plans, policies, procedures, instructions and practices that the licensee implements to assist in securing licensed radioactive material from unauthorized removal or sabotage.

These measures shall include, but are not limited to, the following:

- site security plan
- security awareness program
- personnel trustworthiness and reliability
- protection of prescribed or sensitive information
- inventory control
- access control procedures

3.3.1 Site security plan

For category 1, 2 and 3 sources, technical and administrative measures shall be documented by the licensee in a site security plan, appropriately designated as prescribed information in accordance with sections 21 to 23 of the *General Nuclear Safety and Control Regulations*. The site security plan shall be reviewed by the licensee at least once a year and updated based on changes to the physical or operational security measures or to address any changes within the licensed facility.

Guidance

For information on a site security plan, and for a site security plan template, refer to appendix A, "Sample Site Security Plan".

3.3.2 Security awareness program

All persons with authorized access to sealed sources or prescribed information at the licensee's location (including servicing companies, contractors and building maintenance staff) shall be made aware of the security policies, protocols and practices of the facility. Records of security training and awareness sessions must be retained in accordance with paragraph 36(1)(*d*) and subsection 36(2) of the *Nuclear Substances and Radiation Devices Regulations*. The security awareness program shall be documented and reviewed by the licensee annually. The licensee shall implement an assured process for ensuring new employees participating in security awareness training, and refresher training shall be conducted on a regular basis for existing employees.

Guidance

The security awareness training should include instructions on security practices/procedures to protect sealed sources and prescribed information, and on reporting suspicious events or security incidents (including during transport).

At a minimum, the security awareness program should:

- ensure that staff understand their roles and responsibilities for security
- ensure staff are trained to recognize and report suspicious activity, for example:
    - using false identification
    - individual exhibiting suspicious behavior
    - individual causing an alarm without authorization
    - lost or stolen uniforms or material within the organization
    - unsafe behavior at the workplace
- ensure protection of prescribed and/or sensitive information
- include training on measures for identifying suspicious activity and/or behavioral changes in personnel or contractors

For the security awareness program, the licensee should establish and maintain an overall training policy and initial and continuing training programs, based on the long-term qualifications and competencies required for performing the job, and training goals that acknowledge the critical role of safety and security.

For additional information on establishing a security culture in the organization, refer to the IAEA's *Nuclear Security Culture*, section 3.3 [8].

3.3.3 Personal trustworthiness and reliability

The licensee shall verify the trustworthiness and reliability of all persons who require access to sealed sources at the licensee's location or to prescribed/sensitive information [9] including servicing companies, contractors and building maintenance staff who require access without escort. Personnel who require access to such radioactive material or prescribed/sensitive information to perform job duties, but who are not approved by the licensee, must be escorted by an approved individual. The nature and depth of personnel screening practices [9] shall be based on the category of the radioactive material.

For category 1, 2 and 3 sources, the licensee shall, at a minimum, verify the following information:

a. confirm the identity of personnel from reliable original documentation such as passport or combination of other original documents with photo ID (e.g., valid drivers license, health card or birth certificate)
b. a record emanating from the Canadian Police Information Center or from a police service, showing the result of a criminal records name check (CRNC) on the person
c. the person's employment history, including their educational achievement, and professional qualifications, unless the person has been employed for more than five years at the facility
d. if a person's history cannot be established for at least the last five years, information relating to the trustworthiness of the person including, where available, a CRNC from each country in which the person has resided for one or more years in the last five years

The trustworthiness and reliability verification shall be updated on a regular basis; at a minimum, every five years.

The licensee is responsible for retaining documentation regarding trustworthiness and reliability for the period ending one year after the expiry of the licence in accordance with subsection 28(1) of the *General Nuclear Safety and Control Regulations*. The licensee must permit the CNSC to have access to the trustworthiness and reliability records for review, inspection, or audit purposes.

Alternative to a criminal records name check

If an individual holds one of the following documents or permits, that individual may be exempted from the CRNC as these are considered to be equivalent alternatives:

- Natural Resources Canada (NRCan) Explosive Regulatory Division security screening letter
- Free and Secure Trade Card (FAST) issued by Canada Border Services Agency (CBSA)
- NEXUS Card issued by CBSA
- Firearm Possession and Acquisition Licence (PAL) issued under the *Firearms Act*, S.C. 1995, C.39
- Permis Général issued under the *Québec Explosive Act*, R.S.Q E-22
- a security assessment under the Controlled Goods Program administered by the Controlled Goods Directorate of the Department of Public Works and Government Services Canada

When the individual provides current valid proof of one of these documents or permits to the licensee/employer, the licensee/employer may grant unescorted access to high-risk sealed sources without conducting a CRNC.

Guidance

The licensee's trustworthiness verification program should ensure individuals who have unescorted access to high-risk radioactive sealed sources are trustworthy and reliable, and do not pose an unreasonable risk to the health and safety of persons and security. The licensee should maintain copies of all documents provided by applicants and ensure they have been verified as original. The trustworthiness verification program should be reviewed on a regular basis.

The trustworthiness verification program should apply to:

- individuals with unescorted access to category 1, 2 and 3 sources
- vehicle drivers and those accompanying the transport of category 1 sources
- any individual whose assigned duties provide access to prescribed and/or sensitive information or the handling of category 1 sources (including onsite security officers)

The trustworthiness verification program identifies past actions to help determine an individual's past and current character and reputation in order to provide reasonable assurance of that individual's future reliability. Some indicators that licensees may consider while verifying trustworthiness and reliability include:

- conviction for a serious crime within the past five years (including murder, attempted murder, or indictable offences involving violence)
- impaired performance or dangerous behaviour attributable to psychological or other disorders
- misconduct that warrants criminal investigations or results in arrest or conviction
- indication of deceitful or delinquent behaviour
- attempted or threatened destruction of life or property
- illegal drug use, abuse or distribution
- alcohol abuse disorders
- failure to comply with work directives
- hostility or aggression toward fellow workers or authority
- uncontrolled anger
- violation of safety or security procedures

Note that these indicators are not all-inclusive and they are not intended to be disqualifying factors. Licensees should consider extenuating or mitigating factors. For additional guidance, refer to Appendix B for a process chart of the steps for assessing a person's criminal record.

In cases where:

- gaps exist in the documentation, or CRNC results show either "records match" or "incomplete", the licensee should inform the applicant, and ensure the information is completed and/or accurate
- gaps exist in the individual's history (residence or employment), the licensee should contact the applicant to retrieve all necessary information, and meet with the applicant to clarify any concerns
- it is not possible to obtain background information to cover the last five years, or if significant adverse information arises during the process of the trustworthiness and reliability verification, the licensee should notify the individual in person and give them the opportunity to provide clarifications or explanations
- there are indictable convictions, the licensee should conduct a security interview
    - the criteria used to decide whether a security interview is necessary should include assessing the risk to the high-risk radioactive source(s) or site security
    - the decision to grant, deny or revoke unescorted access to the radioactive material rests with the licensee; the decision should be supported by a management policy that includes a risk-based decision-making process
- CRNC information is unavailable or incomplete, or an indictable conviction exists, fingerprints should be verified through a police service agency (in the area of jurisdiction where the person has resided) or by a trusted third party

Additional information on personnel screening practices can be found in the *Policy on Government Security*, Treasury Board of Canada Secretariat [9].

3.3.4 Protection of prescribed and/or sensitive information

The licensee shall provide protection measures to control access to prescribed information, pursuant to sections 21 to 23 of the *General Nuclear Safety and Control Regulations*, and to prevent loss, illegal use, illegal possession or illegal removal of such prescribed information. This information shall be managed on a "need to know" basis.

Guidance

"Prescribed information" is defined in the *General Nuclear Safety and Control Regulations*, section 21 (see glossary).

The following information is considered to be examples of prescribed information:

- the facility security plan, correspondence related to security, security response measures, contingency plans and transport security plan, if applicable
- the specific location and inventory of sources, installation schematics and security systems including performance testing
- threat and risk assessment and/or vulnerability assessment

Prescribed and/or sensitive information should be:

- protected from unauthorized disclosure and secure when left unattended
- disclosed only to individuals with a "need to know" basis to perform their assigned duties
- stored in a manner that prevents removal or theft

Highly sensitive documents should be stored on a hard medium (diskette, CD-ROM or USB key) or in paper format only, and kept in a secure location that is accessible only to individuals with a "need to know". This information should not be stored on an open or shared network without proper protection.

For prescribed and/or sensitive information, the licensee should:

- use "portable" storage devices (i.e., computer, external hard drive, USB keys) that can be removed and secured
- use storage devices that are "protected" via passwords or encryption, and are only accessible to authorized users via approved cyber security protocols
- protect the confidentiality, availability and integrity of information or documents containing prescribed information

For transportation and transmission of prescribed and/or sensitive information:

- the top right-hand corner of each page of the document should include the security classification level in bold, upper-case letters (i.e., "**PRESCRIBED INFORMATION**")
- the document and the related correspondence may be forwarded to the CNSC by mail, courier, or "secure facsimile"
- electronic transmission (e.g., email) of this information is not acceptable, unless it is encrypted using proper technologies

Prescribed information and documents containing sensitive information that is obsolete or no longer relevant should be shredded or destroyed in accordance with the security rating of the material designated for destruction.

3.3.5 Inventory control

The licensee shall conduct regular inventory checks for detection purposes, to verify that the source(s) are secure and have not been altered or subject to illegal access or unauthorized removal. These inventory checks shall comply with paragraph 36(1)(a) of the *Nuclear Substances and Radiation Devices Regulations*.

Guidance

The licensee should establish and maintain a list of sealed sources under their responsibility. Inventory verification can be used as part of detection measures. Regular inventory checking should consist of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification during onsite movement or transfer, remote observation through closed circuit television (CCTV), or verification of seals or other tamper devices on storage containers and facilities. A process for inventory control should be in place, to ensure a robust verification process.

4. Security Measures for Sealed Sources During Transport

4.1 Vehicle security

For the transport of a category 1 source, the vehicle shall be equipped with:

- a vehicle tracking device that enables the vehicle to be recovered if stolen
- a duress alarm or an equivalent device that is continuously monitored; the licensee shall instruct the alarm monitoring station to alert the appropriate response force (e.g., local law enforcement agency)

For category 1, 2 and 3 sources, the licensee's vehicles shall be equipped with anti-theft devices. The anti-theft devices shall consist of:

- a vehicle disabling device (e.g., starter disabler that prevents the start of the vehicle without a proper key or a similar start device)
- if the vehicle is left unattended, a device that immediately detects unauthorized entry or attack to the vehicle and triggers an audible or visible alarm. If the vehicle operator is not within hearing or visual range of the alarm, the operator shall have the ability to monitor the alarm devices remotely

These anti-theft devices shall be activated automatically or manually by the operator at any time when the vehicle containing the package is left unattended.

While being stored during transportation, the package shall either be stored in a secure container in the vehicle, or in a location that is protected by physical security measures and is continuously monitored when the package is left unattended.

For category 4 and 5 sources, the licensee shall implement prudent management practices by using effective access control and ensuring the security of radioactive material and devices at all times.

Guidance

If a licensee's transport vehicle is left unattended while transporting category 1, 2 and 3 sources, the licensee should have a means to immediately detect, assess and respond to actual or attempted theft or diversion of the sealed sources. An alarm system is an acceptable method. Examples of

acceptable vehicle disabling devices that provide effective delay include trailer hitch locks, wheel locks ("boots"), or a method to disable the engine.

The licensee should ensure a secondary means to protect the vehicle, including a securing mechanism having a similar attack resistance (e.g., chain, locks, and seals).

4.2 Security measures for sealed sources during transport

As the licensee (the consignor) is responsible for the safety and security of sealed sources during transport, the licensee shall ensure the authorized carrier is capable of providing physical security measures for sealed sources while they are in transport or being stored during transportation.

As required by the *Packaging and Transport of Nuclear Substances Regulations*, the licensee shall provide the carrier with the appropriate shipping documents relating to the sealed source. The shipping documents shall include a statement regarding the actions, if any, to be taken by the carrier, and shall also include a description of the security measures for sealed sources. Where more than one category of sources is included in the consignment, the applicable measures shall be based on the more restrictive category.

All packages containing sealed sources of category 1, 2 or 3 shall be protected from unauthorized access, theft or unauthorized removal during transport and temporary storage during transport. The consignee should be notified when, where and by whom such packages are being moved, including tracking numbers and expected arrival times. The licensee, being the consignor, shall contract a carrier with a proven record for the safety and security of dangerous goods while in transport, and shall take the following precautions:

1. The package containing the sealed source shall be stored in a secure container. Packages over 500 kg are considered secure due to the handling difficulties caused by their weight. The secure container does not replace any other packaging or labelling required by any existing regulations. A secure container:

    a. shall be made of steel or any other material that is resistant to a physical attack by handheld tools

    b. shall be equipped with a key, combination padlock or similar locking device that is resistant to an attack using handheld tools

    c. if transported in an open conveyance (e.g., open back of a half-ton truck, flatbed truck), it shall be securely affixed to the vehicle to prevent unauthorized removal of the container

    d. if containing a sealed source with an activity level less than category 3 (see Table A), may be stored in the securely locked trunk or other cargo area of a vehicle while in storage and during transportation

2. During a stopover while being transported, the package shall either be stored in a secure container in the vehicle (as described in list item 1, above), or in a location that is protected by physical security measures (as described in section 3).

3. The vehicle operator shall have on his or her person, at all times, a reliable mobile communication capability (e.g., cell phone) and a list of contact persons and their contact numbers in the event of an emergency situation.

Alternate methodologies that provide a level of physical security equivalent to that described above may be submitted to the CNSC for review, or identified in a licence application or a request to amend a licence.

For transport of category 1 or 2 sources and devices, the licensee shall verify that the carrier:

- uses a package tracking system
- implements methods to ensure trustworthiness and reliability of drivers
- establishes constant control and/or surveillance during transit
- has the capability for immediate communication to summon appropriate response or assistance

For transport of category 3 sources, the licensee shall verify that the carrier:

- implements methods to ensure trustworthiness and reliability of drivers
- maintains constant control and/or surveillance during transit
- has the capability for immediate communication to summon appropriate response or assistance

For transport of category 4 and 5 sources, the licensee shall implement prudent management practices by using effective access control and ensuring the security of radioactive material and devices at all times.

Guidance

Security awareness training should be provided to all individuals engaged in the handling or transport of sealed sources, including refresher training when required.

Before transporting category 1 and 2 sources, all of the carrier's employees who are involved in transporting the sealed sources should have successfully completed security screening for trustworthiness and reliability

The security awareness training should include the items listed for the transport security plan (see section 4.3) and specific information on:

- the identified threats for the conveyance
- security concerns and actions to be undertaken in the event of a security incident during transport

Security devices on the transport vehicles should:

- be inspected regularly for any signs of tampering or deterioration that may adversely affect their designated function
- be tested at least every six months
- be inspected by an authorized person to ensure integrity of the security mechanism on the vehicle used to transport category 1 or 2 sources

For sources in use or in transit, such measures may include a secured or fixed container, or placement of the source container inside a secured storage area (e.g., container chained or bolted to the vehicle). For mobile sources in use, continuous visual surveillance may be a substitute for one or two physical barriers. If a sealed source is temporarily stored while in transit (for example, in a warehouse), equivalent security measures should be applied that are consistent with those security measures discussed above for storage of category 1 and 2 sources.

If packages are transported on an open conveyance, the packages should be secured to the vehicle for safety and security.

4.3 Transport security plan

In addition to the requirements in section 4.2.1, the following requirements apply to category 1 and 2 sources:

- For transport of category 1 sources:
  - the licensee shall implement enhanced security measures and submit a preliminary Transport Security Plan to the CNSC at least 60 days before the anticipated date of shipment, providing all available information, for approval by the Commission Tribunal or a designated officer authorized by the Commission Tribunal
  - the preliminary Transport Security Plan shall be reviewed annually and updated if required
  - a final Transport Security Plan, including the supplementary information unique to each shipment, shall be submitted to CNSC 48 hours before the shipment
- For transport of category 2 sources, the licensee shall implement enhanced security measures and develop a generic Transport Security Plan that shall be implemented and reviewed on a regular basis. The Transport Security Plan should be flexible to address changing threat levels, response protocols to a security event and the protection of sensitive information

For category 1 sources, the Transport Security Plan shall include the following information:

1. the name, quantity, chemical/physical characteristics of the radioactive material
2. role and responsibilities of the licensee's personnel, consignors, carriers
3. mode(s) of transport
4. the proposed security measures
5. measures to monitor the location of the shipment
6. provisions for information security
7. communications arrangements made among the licensee, the carrier and the consignee
8. communications arrangements made with any law enforcement agency along the transportation route
9. the planned route
10. alternate routes to be used in case of an emergency

Guidance

For category 1 sources, the transport security plan should include the following general information:

a. contact information for the licensee or applicant
   - include the complete legal name and business address of the licensee or applicant who is submitting the plan
   - include all relevant contact information, such as telephone number, mobile phone number, and email address

b. the name, quantity, chemical and physical characteristics of each of the sealed sources being transported
   - include a description of the radioactive sealed source and device
   - include the category and quantity of the radioactive sealed source being transported

c. role and responsibilities of the licensee's personnel, consignors, and carriers
   - describe who is responsible for security and the transport security plan (name and title)
   - ensure that security-related information is communicated to the consignors and carriers engaged in the transport of the sealed source(s). If transport is subcontracted, the licensee should ensure contractual arrangements exist for developing the security plan

d. mode(s) of transport
   - describe all types of transport used to convey the sealed source(s) from the time the shipment leaves its originating location until it is delivered at its planned destination
   - include the date, time and location of any planned transfers and the contact information (name, job title, and telephone number) for all persons responsible for ensuring the successful transfer of the sealed sources and for verifying the integrity of the associated shipments

e. proposed security measures
   - describe the measures used to monitor the movement of packages and/or conveyances containing radioactive sealed sources (e.g., global positioning system, vehicle tracking and monitoring system)
   - describe the measures used for escort, security searches, and procedures with response force in case of breakdown or a failure of the shipment to arrive at its destination at the expected time
   - describe the procedures to be followed during any schedule stop, or unscheduled delay during transport

f. measures to monitor the location of the shipment

g. provisions for information security
   - describe how the information will be protected
   - describe how this information will be communicated to individuals who need to know this information to perform their duties

h. the communications arrangements made between the licensee, the carrier, and the consignee
   - describe the communication arrangements between the licensee, the consignor, the operator of the vehicle transporting the radioactive sealed source, and the response force along the transport route
   - describe how the licensee plans to ensure that communication coverage is adequate along the entire route
   - indicate the action to be taken if communication contact with a vehicle carrying a radioactive sealed source is lost

i. communication arrangements made with any police agency along the transportation route
   - the licensee should ensure that all responsible police agencies along the transportation route are notified prior to transporting the shipment
   - the consignor should notify the consignee, in advance, of the shipment's departure time, the mode of transport, the expected delivery time and the allowable delivery period around that delivery time
   - the consignee should notify the consignor of receipt or non-receipt of the shipment within the expected delivery period

j. the planned route
   - if the proposed route is to pass through an urban area, the licensee or applicant should describe the precise route to be taken through the area and how the shipment is to be scheduled to avoid peak traffic times
   - include alternate routes to be used in case of an emergency

Appendix A: Sample Site Security Plan

This appendix provides a list of topics to be considered when developing a site security plan [4].

A threat and risk assessment identifies any potential threats and risks, and reveals possible vulnerabilities at a site. The site security plan is developed to mitigate those threats, and to reduce/eliminate the risks and vulnerabilities. The site security plan includes physical protection measures to protect radioactive sources that are stored, processed, used or transported at the licensed facility.

Introduction

- identify and briefly describe the business, the premises, the number of employees and the location
- include a description of the environment, building and/or facility where the radioactive source is used or stored

Security organization

- include a description of the radioactive sealed source and its use
- identify the security zones (restricted area) and areas accessible by the public in the description of the building
- describe the security protocols during routine and non-routine operations
- identify the senior management personnel and the roles and responsibilities of staff and those responsible for security (including designating a person responsible for maintaining the site security plan)
- provide the details of security arrangements for contractors or employed staff
- provide the details of the management arrangements for the facility, especially where these relate to or involve a responsibility for security of the premises

Security policy

- describe the corporate security policy (if applicable)
- include a copy of the memorandum of understanding (MOU) with the local law enforcement agency

Site plan

- provide a drawing, photograph or other accurate illustration of the site
- include all relevant fence lines, boundaries and facilities
- show the location of all security systems
- show the location of all access and egress points

Perimeter

- describe the perimeter, including, as appropriate, details of fences, gates/barriers, windows, security lighting, perimeter intrusion detection system (PIDS), closed circuit television camera (CCTV) or any other arrangements (such as reception or a gatehouse)
- describe the access and egress points to the site for both pedestrians and vehicles, including access control measures

Access control

- provide the number of onsite employees who are authorized to access the radioactive sources or material (i.e., a list of authorized users and persons with unsupervised access to radioactive substances or material)
- include details on access control systems (e.g., card readers or push-button locks), key or code management, and other general access control procedures
- describe the process for visitors and contractors accessing the facility (e.g., escort policy)
- include details and processes for screening vehicles and searches for weapons and explosive substances

Interior security

- provide information for testing assessment devices (e.g., cameras), access control, detection devices, delay measures, response and communication specific to areas where radioactive sources are located

Storage

- provide a list of buildings, rooms or locations (by name and number or other identifier) where radioactive sources are used, stored or transported
- for each building, room or location, include details on:
  - security arrangements for storage of equipment containing sources
  - means of detecting unauthorized intrusion, either to the equipment or to the storage location
  - processes or procedures for accessing the licensed facility
  - type and categorization of radioactive material

Transportation

- provide a list of vehicles used for the transportation of radioactive sealed sources
- describe the security measures in place for transporting sealed sources, including:
  - security arrangements while sources are being transported
  - means of detecting unauthorized removal of equipment
  - security processes or procedures to be applied while sources are being transported

Security of information

- describe the arrangements for the protection of sensitive information regarding the location, nature, storage and movement of radioactive sources
- all correspondence related to security (including the site security plan) is marked "**PRESCRIBED INFORMATION**" and as such, it must be safeguarded and labelled pursuant to sections 21 to 23 of the *General Nuclear Safety and Control Regulations*
- if prescribed information is stored on a company server connected to the Internet, ensure that consideration is given to potential threat and vulnerabilities from IT systems

Background checks to determine trustworthiness and reliability

- describe the arrangements for verifying the identity and reliability of staff having access to high risk radioactive sources
- describe the arrangements for verifying the identity and reliability of persons providing security protection for the facility, including contractors or building maintenance staff

Maintenance, repair and testing of security systems

- describe the arrangements for the maintenance and testing of all security systems
- include information on compensatory measures, performance testing and reliability verification of security systems
- describe the process for evaluating the effectiveness of the security maintenance plan, including the frequency for updating the plan in accordance with CNSC expectations (e.g., semi-annual testing)

Contingency and security response plans

- provide details on the security procedures and instructions to address security measures to respond to loss, theft, destruction, malevolent acts or any other security incident involving radioactive substances or material
- include information on emergency plans and event reporting
- describe agreements with offsite responders (e.g., police) for alarm response protocol or other security incidents
- include procedures that address an increased threat level with details on any compensatory measures that may be required

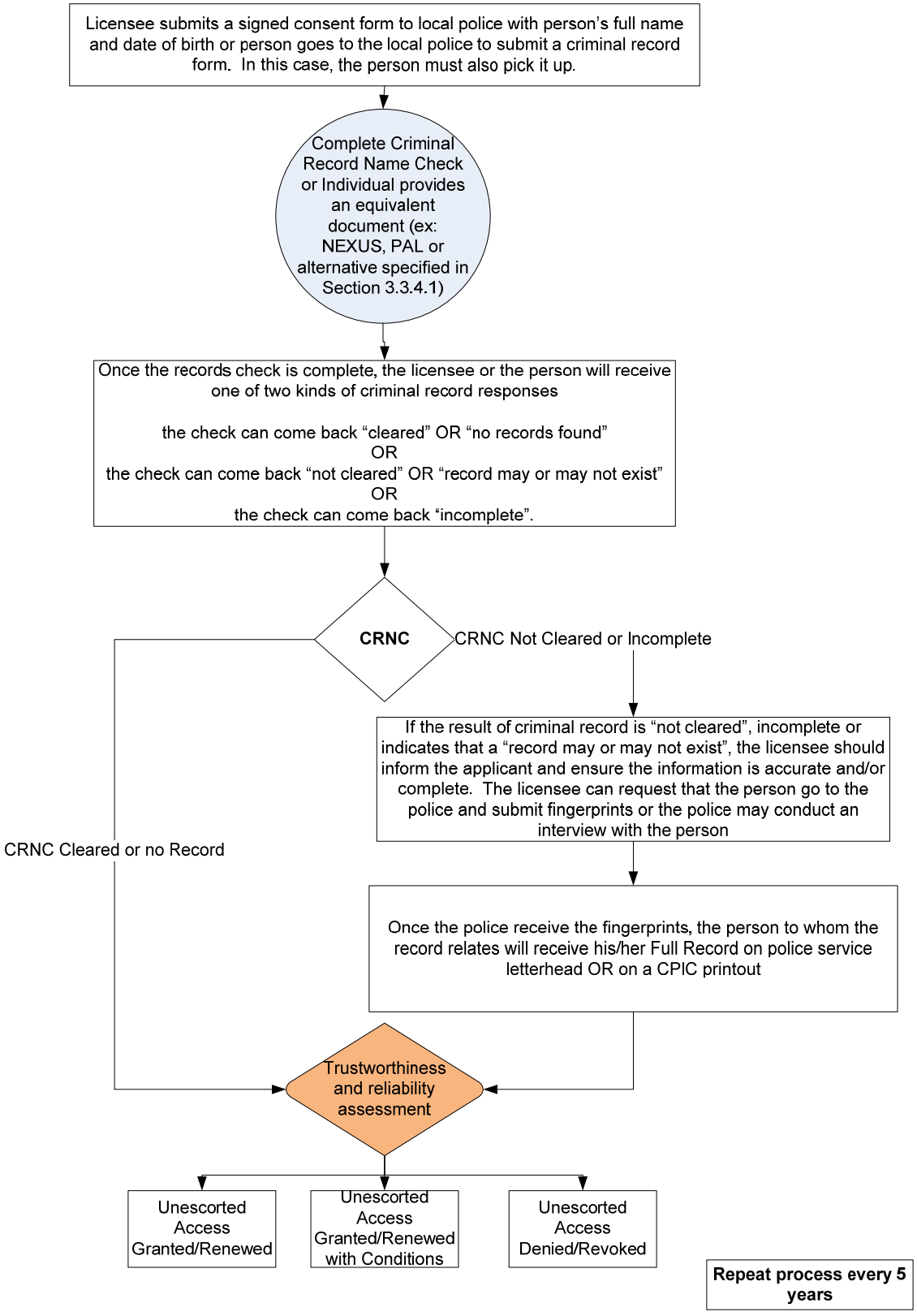
Security awareness program

- describe the security awareness program
- include any instructions given to employees on security measures
- include any restrictions concerning access, use, storage or transportation of radioactive substances or material (including restrictions on contractors, building maintenance staff, and temporary employees)

References, procedures and security instructions

- include references to existing regulations or standards and/or any procedures related to security

Appendix B: Example of a Criminal Records Name Check Process



Appendix C: Application of REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources* for Typical Uses of Sealed Sources

This appendix provides information on typical uses of sealed sources and their respective security level. The following table is provided for guidance purposes only. The application of the security level may vary depending on the source, the aggregate quantities, the threat level, and the risks associated with the manner and location in which the sealed source is used.

Legend:
Y Yes
P Prudent management practice

Table C: Application of REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources* for typical uses of sealed sources

Practice	Security level	Paragraph of *Security of Nuclear Substances: Sealed Sources* (requirements)															
		Technical security measures							Administrative security measures						Transport measures		
		3.1	3.2.1	3.2.2	3.2.3	3.2.4	3.2.5	3.2.6	3.2.7	3.3.2	3.3.3	3.3.4	3.3.5	3.3.6	4.1	4.2	4.3
Irradiators: pool type, sterilization and food preservation	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Processing/manufacturer	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Irradiators: self-shielded	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Irradiators: blood/tissue	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Multi-source teletherapy (gamma knife)	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Teletherapy	1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Industrial radiography	2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Well logging	2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Brachytherapy - high dose rate or pulsed dose rate	2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	P	P
Conveyor gauges	3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	P	P
Blast furnace gauges	3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	P	P
Dredger gauges	3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	P	P
Spinning pipe gauges	3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	P	P
Brachytherapy - low dose rate	4	Y	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Thickness gauges	4	Y	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Fill-level, thickness gauges	4	Y	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Moisture detectors	4	Y	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Density gauges	4	Y	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Practice	Security level	Paragraph of *Security of Nuclear Substances: Sealed Sources* (requirements)															
		Technical security measures							Administrative security measures						Transport measures		
		3.1	3.2.1	3.2.2	3.2.3	3.2.4	3.2.5	3.2.6	3.2.7	3.3.2	3.3.3	3.3.4	3.3.5	3.3.6	4.1	4.2	4.3
Moisture/density gauges	4	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**
Static eliminators	4	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**
X ray fluorescence analyzers	5	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**
Electron capture detectors	5	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**
Brachytherapy: low dose rate eye plaques and permanent implants	5	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**
Positron Emission Tomography (PET) checking	5	**Y**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**	**P**

Glossary

authorized access
Access that is granted in writing by the licensee.

category 1 source
Sources that, if not safely managed or securely protected, would be likely to cause permanent injury to a person who handled them, or were otherwise in contact with them for more that a few minutes. It would probably be fatal to be close to this amount of unshielded material for a period of a few minutes to an hour. These sources are typically used in practices such as radiothermal generators, irradiators and radiation teletherapy.

category 2 source
Sources that, if not safely managed or securely protected, could cause permanent injury to a person who handled them, or were otherwise in contact with them, for a short time (minutes to hours). It could possibly be fatal to be close to this amount of unshielded radioactive material for a period of hours to days. These sources are typically used in practices such as industrial gamma radiography or oil well logging.

category 3 source
Sources that, if not safely managed or securely protected, could cause permanent injury to a person who handled them, or were otherwise in contact with them, for some hours. It could possibly – although it is unlikely – be fatal to be close to this amount of unshielded radioactive material for a period of days to weeks. These sources are typically used in practices such as fixed industrial gauges involving high activity sources (for example, high dose rate brachytherapy, level gauges, dredger gauges, conveyor gauges and spinning pipe gauges).

category 4 source
Sources that are very unlikely to permanently injure anyone. However, this amount of unshielded radioactive material, if not safely managed or securely protected, could possibly – although it is unlikely – temporarily injure someone who handled it or was otherwise in contact with it, or who was close to it for a period of many weeks.

category 5 source
Sources that could not permanently injure someone.

criminal records name check (CRNC)
A search used to determine if a person has a criminal record. The search can be based on name and date of birth or – for much greater assurance – on fingerprints, for positive identification.

designated officer
A person designated as a designated officer under section 37 of the *Nuclear Safety and Control Act* (NSCA).

encapsulated source
The radioactive material is permanently sealed in a capsule or closely bounded in a solid form.

handheld tools
Tools and equipment that may be used by an adversary to penetrate a security system or barrier. These tools may include hand tools such as bolt-cutters, pliers or hacksaw blades, power tools, burn bars or cutting torches, as well as any tool or equipment located at the facility.

licensing basis
A set of requirements and documents for a regulated facility or activity comprising:
- the regulatory requirements set out in the applicable laws and regulations
- the conditions and safety and control measures described in the facility‘s or activity’s licence and the documents directly referenced in that licence
- the safety and control measures described in the licence application and the documents needed to support that licence application

prescribed information
Information that concerns any of the following, including a record of that information, is prescribed information for the purposes of the NSCA:
- a nuclear substance that is required for the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device, including the properties of the nuclear substance
- the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device
- the security arrangements, security equipment, security systems and security procedures established by a licensee in accordance with the NSCA, the regulations made under the NSCA or the licence, and any incident relating to security
- the route or schedule for the transport of Category I, II or III nuclear material, as defined in section 1 of the *Nuclear Security Regulations*

Information that is made public in accordance with the NSCA, the regulations made under the NSCA or a licence is not prescribed information for the purposes of the NSCA.

prudent management practices
Include ensuring that sealed sources are secured to prevent illegal use, theft or sabotage, and that a periodic inventory is carried out to ensure sealed sources are at their designated location and are secure.

sabotage
Any deliberate act or omission, directed against a nuclear facility or nuclear substances, that:
- endangers or is likely to endanger the health and safety of any person, or
- results or is likely to result in contamination of the environment

In the context of security measures for sealed sources, sabotage includes any deliberate act or omission directed against a sealed source.

sealed source
A radioactive nuclear substance in a sealed capsule or in a cover to which the substance is bonded, where the capsule or cover is strong enough to prevent contact with or the dispersion of the substance under the conditions for which the capsule or cover is designed.

storage
The holding of radioactive sources in an area that provides for their containment with the intention of retrieval.

temporary storage
Storage during the transportation cycle when a sealed source is unattended.

UL
Underwriters Laboratories (UL) is a global independent safety science company offering expertise across five key strategic businesses: product safety, environment, life and health, university and verification services.

ULC
Underwriters Laboratories of Canada (ULC) is an independent product safety testing, certification and inspection organization.

unsealed source
A source other than a sealed source. Can be in liquid or solid form, and is commonly used in medical diagnostic and therapeutic treatments, as well as in laboratory research applications.

use-type
The purpose for which the licence has been issued.

vehicle
Any means of air, water or land transport, and includes railway equipment within the meaning assigned to that expression by subsection 4(1) of the *Railway Safety Act*. For the purposes of this regulatory document, a road vehicle (including an articulated vehicle such as a trailer and semi-trailer combination), railroad car or railway wagon. Each trailer is considered to be a separate vehicle.

References

1. International Atomic Energy Agency (IAEA), *Code of Conduct on the Safety and Security of Radioactive Sources,* Vienna, 2004 http://www-pub.iaea.org/MTCD/Publications/PDF/Code-2004_web.pdf

2. IAEA, Safety Guide RS-G-1.9, *Categorization of Radioactive Sources*, 2005 http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1227_web.pdf

3. IAEA, TECDOC-1344, *Categorization of Radioactive Sources*, Revision of TECDOC-1191, *Categorization of Radiation Sources*, 2003 http://www-pub.iaea.org/MTCD/Publications/PDF/te_1344_web.pdf

4. IAEA, TS-R-1, *Regulations for the Safe Transport of Radioactive Material*, 1996 edition (revised) http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1098_scr.pdf

5. IAEA, TECDOC-1355, *Security of Radioactive Sources – Interim Guidance for Comment*, 2003 http://www-pub.iaea.org/MTCD/Publications/PDF/te_1355_web.pdf

6. ASTM F2548-06, *Standard Specification for Expanded Metal Fence Systems for Security Purposes*, ASTM International, West Conshohocken, PA, 2006, DOI: 10.1520/F2548-06 http://www.astm.org/DATABASE.CART/HISTORICAL/F2548-06.htm

7. Natural Resources Canada, *Guidelines for Jet Perforating Gun Assembly Facilities*, 2008

8. IAEA, Nuclear Security Series No. 7, implementing guide, *Nuclear Security Culture*, Vienna, 2008 http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

9. Treasury Board of Canada Secretariat, Government of Canada, *Policy on Government Security*, July 2009. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text

Additional Information

The following documents contain additional information that may be of interest to persons involved in security measures for sealed sources.

- Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), *Code of Practice for the Security of Radioactive Sources*, Radiation Protection Series Publication No. 11, January 2007

- Canadian Nuclear Safety Commission, INFO-9999-4 (E) Revision 2, *Working Safely with Nuclear Gauges*, Ottawa, 2007

- IAEA, INFCIRC/225/Rev 5, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, Nuclear Security Series No. 13, 2011 (draft)

- IAEA, INFCIRC/663, *Code of Conduct on the Safety and Security of Radioactive Sources and the Supplementary Guidance on the Import and Export of Radioactive Sources*, 2005

- IAEA, TECDOC-953, *Method for the Development of Emergency Response Preparedness for Nuclear or Radiological Accidents*, 1997

- IAEA, Nuclear Security Series No. 9, implementing guide, *Security in the Transport of Radioactive Material*, 2008

- IAEA, Nuclear Security Series No. 11, *Security of Radioactive Sources*, 2009

- IAEA, Nuclear Security Series No. 14, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*, 2011

- IAEA, TECDOC-1276, *Handbook on the physical protection of nuclear materials and facilities*, 2002

- National Counter Terrorism Security Office (UK), *Security requirements for radioactive sources*, restricted document, April 2011

- North Atlantic Treaty Organisation (NATO) Science for Peace and Security Series - C: Environmental Security, *International Approaches to Securing Radioactive Sources Against Terrorism*, edited by W. Duncan Wood and Derek M. Robinson, Springer Science+Business Media, 2009

- United States Nuclear Regulatory Commission (USNRC), *Increased controls for licensees that possess sources containing radioactive material quantities of concerns*, 2009

CNSC Regulatory Document Series

Facilities and activities within the nuclear sector in Canada are regulated by the Canadian Nuclear Safety Commission (CNSC). In addition to the *Nuclear Safety and Control Act* and associated regulations, these facilities and activities may also be required to comply with other regulatory instruments such as regulatory documents or standards.

Effective April 2013, the CNSC's catalogue of existing and planned regulatory documents has been organized under three key categories and twenty-five series, as set out below. Regulatory documents produced by the CNSC fall under one of the following series:

1.0 Regulated facilities and activities

Series
- 1.1 Reactor facilities
- 1.2 Class IB facilities
- 1.3 Uranium mines and mills
- 1.4 Class II facilities
- 1.5 Certification of prescribed equipment
- 1.6 Nuclear substances and radiation devices

2.0 Safety and control areas

Series
- 2.1 Management system
- 2.2 Human performance management
- 2.3 Operating performance
- 2.4 Safety analysis
- 2.5 Physical design
- 2.6 Fitness for service
- 2.7 Radiation protection
- 2.8 Conventional health and safety
- 2.9 Environmental protection
- 2.10 Emergency management and fire protection
- 2.11 Waste management
- 2.12 Security
- 2.13 Safeguards and non-proliferation
- 2.14 Packaging and transport

3.0 Other regulatory areas

Series
- 3.1 Reporting requirements
- 3.2 Public and Aboriginal engagement
- 3.3 Financial guarantees
- 3.4 Commission proceedings
- 3.5 Information dissemination

Note: The regulatory document series may be adjusted periodically by the CNSC. Each regulatory document series listed above may contain multiple regulatory documents. For the latest list of regulatory documents, visit the CNSC's Web site at nuclearsafety.gc.ca/regulatory-documents