Canada's Nuclear Regulator

Security

Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material

REGDOC-2.12.3, Version 2

DRAFT

June 2018

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Security of Nuclear Substances: Sealed Sources and Category I, II, and III Nuclear Material, Version 2
Regulatory document REGDOC-2.12.3, Version 2

Cat. No. XXXXX
ISBN XXXXX

Également publié en français sous le titre : La sécurité des substances nucléaires : sources scellées et matières nucléaires de catégories I, II et III, version 2

Document availability

This document can be viewed on the CNSC website. 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, ON K1P 5S9
CANADA

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Fax: 613-995-5086
Email: cnsc.info.ccsn@canada.ca
Website: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn
Twitter: @CNSC_CCSN
LinkedIn: linkedin.com/company/cnsc-ccsn

Publishing history
[Month year] Version x.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 also be found on the CNSC's website.

Part A of Regulatory document REGDOC-2.12.3, version 2, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material*, 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.

Part B of this document also provides information and guidance on how to comply with the minimum security measures, including measures related to transport vehicles, containers and security plans. For sealed sources, 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).

This document sets out guidance to help applicants for a Canadian Nuclear Safety Commission (CNSC) licence in respect of Category I or II nuclear material – other than a licence to transport – or a nuclear facility consisting of a nuclear reactor that may exceed 10 MW thermal power during normal operation, to prepare and submit the security information to be included with the application, pursuant to the *Nuclear Safety and Control Act*. This document also sets out guidance to help applicants for a CNSC licence to transport Category I, II or III nuclear material to prepare and submit a "written transportation security plan" that meets the requirements of section 5 of the *Nuclear Security Regulations*. Category I, II and III nuclear material are defined in appendix E to this guide.

This document supersedes CNSC guidance documents G-208, *Transportation Security Plans for Category I, II, or III Nuclear Material*, and G-274, *Security Programs for Category I or II Nuclear Material or Certain Nuclear Facilities*, and REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources*.

Part A of this document applies to sealed radioactive sources (encapsulated or solid) and does not apply to unsealed radioactive substances. Part A of 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 I to V sources are used as defined in the IAEA's *Code of Conduct on the Safety and Security of Radioactive* [1], IAEA Safety Guide RS-G-1.9, *Categorization of Radioactive Sources* [2] or IAEA/TECDOC-1344, *Categorization of Radioactive Sources* [3].

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.

Guidance contained in this document exists to inform the applicant, to elaborate further on requirements or to provide direction to licensees and applicants on how to meet requirements. It also provides more information about how CNSC staff evaluate specific problems or data during their review of licence applications. Licensees are expected to review and consider guidance; should they choose not to follow it, they should explain how their chosen alternate approach meets regulatory requirements.

For existing facilities: the requirements contained in this document do not apply unless they have been included, in whole or in part, in the licence or licensing basis.

A graded approach, commensurate with risk, may be defined and used when applying the requirements and guidance contained in this regulatory document. The use of a graded approach is not a relaxation of requirements. With a graded approach, the application of requirements is commensurate with the risks and particular characteristics of the facility or activity.

An applicant or licensee may put forward a case to demonstrate that the intent of a requirement is addressed by other means and demonstrated with supportable evidence.

The requirements and guidance in this document are consistent with modern national and international practices addressing issues and elements that control and enhance nuclear safety. In particular, they establish a modern, risk-informed approach to the categorization of accidents – one that considers a full spectrum of possible events, including events of greatest consequence to the public.

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

Document Title

1. Introduction

1.1 Purpose

Part A of Regulatory document REGDOC-2.12.3, version 2, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material*, 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 or transport, or being stored during transportation.

Part B of this document sets out guidance to help applicants prepare and submit the security information to be included with an application for a licence in respect of Category I or II nuclear material or a nuclear facility. It also provides guidance for applicants to prepare a "written transportation security plan" with respect to a licence to transport Category I, II or III nuclear material.

1.2 Scope

Part A of this document describes the minimum security measures required for the use, storage and transport 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.

Part A 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 sources" to "category 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).

Part B of the document describes the security measures for the storage and/or transport of nuclear materials. It describes the information that should be present in a licensee's security program description or transportation security plan. The document also provides details on how these plans should be handled in order to meet confidentiality and national security requirements.

Part B applies to applicants for a licence with respect to Category I, II or III nuclear material as well as nuclear facilities consisting of a nuclear reactor. In this document, the terms Category I, II and III nuclear material are used as defined in the *Nuclear Security Regulations* (NSR) (see also appendix E).

Other federal requirements related to the transport of Category I, II or III nuclear material, such as those pertaining to packaging, documentation and safety markings, can be found in the *Packaging and Transport of Nuclear Substances Regulations* 2015 and the *Transportation of Dangerous Goods Regulations*.

The *Packaging and Transport of Nuclear Substances Regulations, 2015* (PTNSR 2015) apply to consignors, consignees and carriers (both licensees and non-licensees). REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material* 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 complies with while the sealed sources are in transport or being stored during transportation.

For sealed sources, 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).

1.3 Relevant legislation

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)(e), (g) and (h) of the *General Nuclear Safety and Control Regulations* (GNSCR), which state that "an application for a licence shall contain the following information:…
  (e) the proposed measures to ensure compliance with the Radiation Protection Regulations, the *Nuclear Security Regulations* and the *Packaging and Transport of Nuclear Substances Regulations, 2015*…
  (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"

- paragraph 3(1.1)(b) of the GNSCR, which states that "the Commission or a designated officer authorized under paragraph 37(2)(c) of the Act, may require any other information that is necessary to enable the Commission or the designated officer to determine whether the applicant … will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed"

- paragraphs12(1)(c), (g), (h) and (j) of the GNSCR, which 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 GNSCR, which define prescribed information and provide details on which persons may possess, transfer, import, export, use or disclose prescribed information

- subsection 28(1) of the GNSCR, which 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"

- paragraphs36(1)(a) and (d), and subsection 36(2) of the *Nuclear Substances and Radiation Devices Regulations*, which 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 3 of the NSR, which requires that applications for licences for Category I, and II nuclear material or nuclear power plants contain the following security information:
  "(a) a copy of the arrangements referred to in section 35;
  (b) the site plan referred to in section 16;
  (c) a description of the proposed security equipment, systems and procedures;
  (d) a description of the proposed on-site and off-site communications equipment, systems and procedures;
  (e) a description of the proposed structure and organization of the nuclear security officer service, including the duties, responsibilities and training of nuclear security officers;;
  (f) the proposed plan and procedures to assess and respond to breaches of security; and
  (g) the current threat and risk assessment."

- section 4 of the NSR requires that an application for a licence in respect of Category III nuclear material, other than a licence to transport, shall contain, in addition to the information required by section 3 of the *Nuclear Substances and Radiation Devices Regulations*, a description of the measures to be taken to ensure compliance with subsection 7(3) and sections 7.1 and 7.2.

- Section 5 of the NSR, which requires that the application for a licence to transport Category I, II and III nuclear material contain, in addition to any other information required by section 7 of the PTNSR 2015, a "written transportation security plan that includes:
  (a) the name, quantity, radiation level in Gy/h, chemical and physical characteristics and isotopic composition of the nuclear material;
  (b) a threat assessment consisting of an evaluation of the nature, likelihood and consequences of acts or events that may place prescribed information or nuclear material at risk;
  (c) a description of the conveyance;
  (d) the proposed security measures;
  (e) the communication arrangements made among the licensee, the operator of the land vehicle transporting the nuclear material, the recipient of the material and any response force along the route;
  (f) the arrangements made between the licensee and any offsite response force along the route;

(g) the planned route; and
(h) the alternate route to be used in case of an emergency."

- paragraph 3 (i) of the *Class I Nuclear Facilities Regulations*, which refers applicants for a licence in respect of a nuclear facility consisting of a nuclear power plant, to section 3 of the NSR

- paragraph 6(1) of the *Class I Nuclear Facilities Regulations*, which stipulates that an application for a licence to operate a Class I facility shall contain, in addition to the information required by section 3 of the same regulations, information on the proposed measures to prevent acts of sabotage or attempted sabotage at the nuclear facility, including measures to alert the licensee to such acts

- section 7 of the PTNSR 2015, which sets out the information required in an application for a licence to transport a nuclear substance

- subsection 29(1) of the PTNSR 2015, which states that "every consignor of radioactive material must include in the transport documents for the consignment the particulars of consignment that are required by the IAEA Regulations [4], which particulars must be clearly and indelibly printed."

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*, 2012 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, Nuclear Security Series 14, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities*, 2011 [10]
- IAEA Nuclear Security Series No. 9, Implementing Guide, *Security in the Transport of Radioactive Material*, 2008
- IAEA, Nuclear Security Series No. 11, Implementing Guide, *Security of Radioactive Sources*

Part A – Sealed Sources

2. Background

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, 2015* (PTNSR 2015)
- 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 low-risk sealed sources, this document provides prudent management practices for managing those categories.

In September 2003, the International Atomic Energy Agency (IAEA) approved the *Code of Conduct on the Safety and Security of Radioactive Sources* [1]. 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 and Category I, II and III Nuclear Material* 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, 2015* apply to consignors, consignees and carriers. However, subcontractors are not licensed by the 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 or nuclear material, during storage, or storing them while in transit.

REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and Category I, II, and III Nuclear Material*, reflects the security goals of United Nations specialized agencies and programs – including the International Maritime Organization, the International Civil Aviation Organization 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.

2.1 Application

Part A applies to sealed sources and radionuclides identified in Table 1. 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 the protection of the health and safety of persons and the environment from the dangers associated with radioactive sources.

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 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 1 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 1: Activities corresponding to threshold 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	1,620	0.6	16	0.06	1.6
Americium-241 / Beryllium (^{241}Am/Be)	60	1,620	0.6	16	0.06	1.6
Californium-252 (^{252}Cf)	20	540	0.2	5.4	0.02	0.5
Cesium-137 (^{137}Cs)	100	2,700		27	0.1	2.7
Cobalt-60 (^{60}Co)	30	810	0.3	8.1	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				
Iridium-192 (^{192}Ir)	80	2,160	0.8	22	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	1,081,000	400	11,000		1,100
Radium-226 (^{226}Ra)	40	1,080	0.4	11	0.04	1.1
Selenium-75 (^{75}Se)	200	5,400		54	0.2	5.4
Strontium-90 (^{90}Sr) / Yttrium-90 (^{90}Y)	1,000	27,000				
Thulium-170 (^{170}Tm)	20,000	540,540	200	5,400		540
Ytterbium-169 (^{169}Yb)	300	8,100		81	0.3	8.1

2.2.1 Thresholds for the activity levels

The materials and thresholds in Table 1 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 G-1.9, *Categorization of Radioactive Sources* [2] provides the methodology for the development of the *Code of Conduct* thresholds.

The IAEA 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.

2.2.2 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 ertified 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 security category. This is done by adding the actual sealed source activities of the sources and determining the category from Table 1. 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 or use, 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
- credible
- mitigation

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

Table 2: 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	ory 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 3.2.1 to 3.2.7.

Pursuant to paragraphs 3(1)(g) and 3(1)(h) of the *General Nuclear Safety and Control Regulations*, the licensee shall include in their application the proposed measures respecting control of access to the site of the licensed activity, as well as the proposed measures to prevent the loss or illegal use, possession or removal of the licensed materials.

3.2.1 Thresholds for the activity levels

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

- 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.

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 1, 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 1, 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.

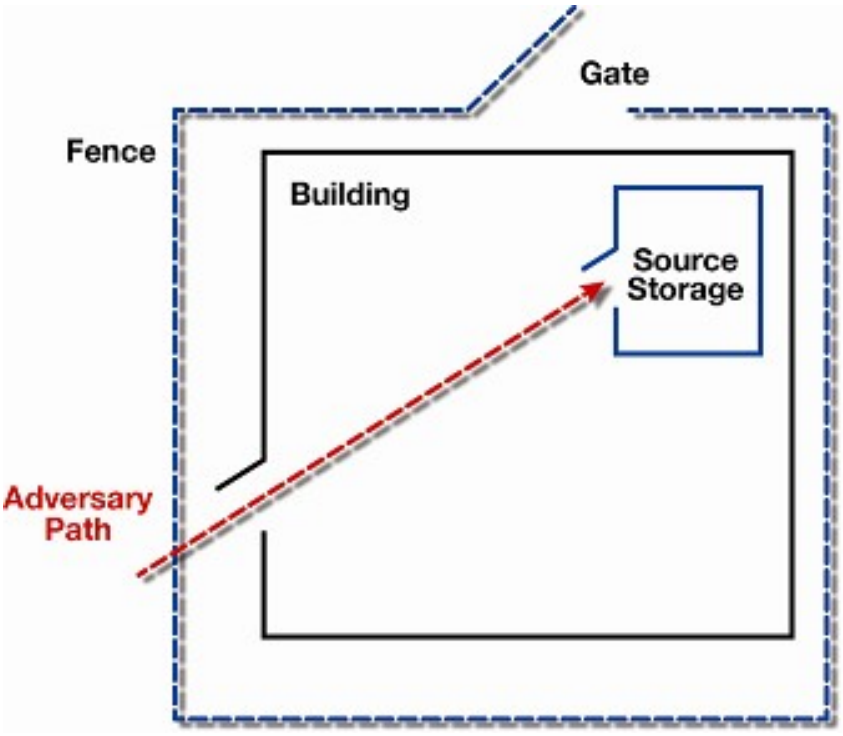
For situations where radioactive sources are used or stored in proximity to explosives, a minimum separation of 3 metres must be maintained between the radioactive sources and all explosive material, as required in section 13 of the *Guidelines for Jet Perforating Gun Assembly Facilities* [7].

Guidance

Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls and vaults are commonly used for storage of 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 UL 437 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 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 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 measure

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:

1. confirm the identity of personnel from reliable original documentation such as passport or combination of other original documents with photo ID (e.g., valid driver's license, health card or birth certificate)
2. 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
3. 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
4. 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 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 Measure 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, 2015*, 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 1), 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 or a designated officer authorized by the Commission
  - 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 sealed sources (e.g., global positioning system, vehicle or package 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

Part B – Nuclear Materials

5. Background

Nuclear material is 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 Regulations*, *Nuclear Substances and Radiation Devices Regulations* and the *Radiation Protection Regulations*.

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

- Canadian Nuclear Safety Commission (CNSC), *Packaging and Transport of Nuclear Substances Regulations, 2015*
- Transport Canada, *Transportation of Dangerous Goods Regulations*

This document uses a graded approach for the security of nuclear material. There are three levels of nuclear material (categories I through III). The guidance provided in this part of the document is graded to the risk posed by the category of nuclear material.

5.1 Application

Part B applies to Category I, II and II nuclear material as defined in appendix E (taken from the *Nuclear Security Regulations* and their schedule).

6. Security Measures

This section provides guidance on the security information that should typically be included with the application for a licence in respect of Category I or II nuclear material — other than a licence to transport —, or a nuclear facility consisting of a nuclear reactor that may exceed 10 MW thermal power during normal operation.

Applicants may consolidate this security information in the security program description. The inclusion with the licence application of such a document, which follows the recommendations of appendix D and which adopts the subject headings of the following sections, will assist CNSC review and processing of the application.

Throughout the security program description, applicants should, whenever possible, name the key persons involved, provide their position titles, and describe their associated roles, responsibilities, authorities and accountabilities.

Sections 6.1 to 6.3 detail the information that should be included in the security program description.

6.1 General information for the security program description

6.1.1 Administrative information

The security program description should contain:

- the complete legal name and business address of the applicant
- the complete names and addresses of three individuals who are to be authorized to act as emergency contacts for the licensee
- the telephone and fax numbers, or email addresses, at which the applicant and the emergency contacts may be contacted
- a description of the licence application to which the security information pertains

6.1.2 Site or facility location and relevant features

Pursuant to section 16 of the *Nuclear Security Regulations* (NSR), a site plan as referred to in paragraph 3(b) of the NSR shall indicate, where applicable, the location of:

- the perimeter of the proposed nuclear facility referred to in paragraph 2(b) of the NSR
- the proposed barrier to enclose every proposed protected area
- the proposed protected areas
- the proposed unobstructed areas that meet the requirements set out in section 10 of the NSR
- the proposed structure or barrier to enclose every proposed inner area
- the proposed inner areas
- the proposed vital areas

Guidance

The security program description should contain an accurate site location, specified in terms of its coordinates (longitude and latitude), and described by a site drawing, done to scale, indicating its features and the surrounding topography. Topographical details, including all access roads, all rail, water and air access routes, the locations of the nearest communities and the natural features of the area should be included. Where necessary, provide written descriptions to support the illustrations.

The security program description should indicate, as applicable, the following additional information:

- the location of any proposed security post that is to be fixed
- any proposed route that is to be patrolled by mobile security forces
- the location of the security monitoring room
- the location of any other secondary security monitoring room outside the inner area
- any other feature that is pertinent to the maintenance of nuclear security

6.1.3 Applicant's corporate security policy

The security program description should include a description of the applicant's existing, or proposed, corporate security policy.

6.2 Technical security measures

Technical security measures for nuclear material or facilities should include measures to:

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

Technical security measures 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 should provide details for the following measures:

- access and identification systems
- access controls
- protected and inner areas
- security monitoring rooms
- communication equipment
- security systems, technical devices and equipment

For cyber security for nuclear power plants and small reactor facilities, the licensee cyber security program should follow CSA standard N290.7-14.

6.2.1 Access and identification systems

The proposed identification badge or access card system for identifying employees, contractors and visitors, and for controlling their entry to protected or inner areas, should be described. This description should include the information that is to appear on each type of proposed identification badge or access card, such as a colour code, photo, security clearance, name, personal description, expiration date and entry restriction.

The security program description should provide a description of the proposed system for issuing, accounting for and storing identification badges or access cards, and for keeping relevant records.

The proposed measures for wearing and displaying identification badges or access cards while on the site of the activity to be licensed should be provided. Procedures for surrendering an identification badge or access card when terminating employment or leaving the site should be included in the description.

6.2.2 Access control

In accordance with paragraph 3(1)(g) of the *General Nuclear Safety and Control Regulations* (GNSCR), the proposed measures to control access to the site of the activity to be licensed and Category I or II nuclear material shall be provided.

Access devices and access information

Access devices and access information that could be used to enter or exit from protected or inner areas should be described. This should include the make, type, design, and manipulation and pick-resistant features, for each device type. Access devices and access information could include:

- keys
- locks
- lock combinations
- card keys
- passwords
- biometric identification systems

Methods or procedures to control access devices or access information should be proposed, including procedures to control the custody and use of keys to enter protected or inner areas. These procedures should include the response to any loss or theft of such keys or other access devices and the precautions to be taken when an employee with access devices or access information terminates employment.

Vehicles

The proposed methods or procedures to control all points of vehicle movement to and from protected or inner areas should be described. This description should include:

- written procedures to help nuclear security officers identify vehicles authorized to enter protected or inner areas
- proposed procedures for escorting vehicles or conducting vehicle searches at entry or exit points

Procedures for both normal and emergency conditions should be provided.

Packages and equipment

The proposed methods or procedures to control all points of access whereby packages and equipment could enter a protected or inner area under normal and emergency conditions should be provided. The description should include:

- written procedures to help nuclear security officers identify the packages and equipment that are to be allowed into protected or inner areas
- proposed procedures for tagging or authorizing packages and equipment, or for implementing searches upon entry or exit

6.2.3 Protected and inner areas

Protected areas

The security program description should set out the measures proposed for meeting the requirements concerning the protected areas that are stated in sections 9, 10 and 11 of the NSR, such as:

- physical barriers, including entry portals, exit portals and security posts, and all proposed intrusion-detection devices that are to be located at the boundaries to, or in, any proposed protected area
- equipment, including illumination and assessment devices, to detect and assess the cause of an annunciating alarm in any protected area
- the unobstructed area that is to surround any proposed protected area

The proposed entry and exit control procedures for persons who are authorized, pursuant to subsection 17(3) of the NSR, to access a protected area when accompanied by an authorized escort, should be described, including:

- the procedures pertaining to authorizations and identification requirements, badges and records
- the procedures to be followed by escorts

- the procedures to establish who may be authorized to escort
- the procedures to establish the training and qualifications required of escorts
- the allowable ratio of visitors to escorts during the activity to be licensed

Entry and exit control procedures for persons who are authorized, pursuant to subsection 17(2) of the NSR, to access a protected area unescorted, including the procedures pertaining to identification requirements, badges and records, should be described. Measures to meet the requirements concerning protected areas that are stated in sections 25, 26 and 27 of the NSR, including any related provision for searching persons for concealed firearms, explosives or any other weapon that could be used to commit a crime, should be provided.

The location of all emergency exits from any proposed protected area should be provided, along with the security measures at said emergency exits, under both emergency and non-emergency conditions.

Vital areas

The proposed measures to meet the requirements concerning vital areas that are stated in section 14.1 of the NSR should be provided.

Inner areas

The proposed location and function of any inner area that, pursuant to section 12 of the NSR, is to be located within a protected area, should be described. Measures to meet the requirements concerning the inner areas referred to in sections 13 and 14 of the NSR should be provided, including:

- physical barriers and all intrusion-detection devices that are to be located at the boundaries to, or in, any proposed inner area
- equipment, including illumination and assessment devices, to detect and assess the cause of an annunciating alarm in any inner area

Entry and exit control procedures for persons who are authorized, pursuant to section 20 of the NSR, to enter an inner area unescorted, should be provided. The description should include the procedures pertaining to authorizations and identification requirements, badges and records.

The security program description should detail how requirements concerning inner areas, as stated in sections 25, 26 and 27 of the NSR, are to be met. Provisions related to searching persons for concealed firearms, explosives or any other weapon that could be used to commit a crime should be included.

The location of all emergency exits from any proposed inner area should be provided, along with the security measures at said emergency exits, under both emergency and non-emergency conditions.

6.2.4 Security monitoring rooms, and onsite and offsite communications equipment, systems and procedures

Security monitoring rooms

The security program description should indicate how the proposed security monitoring room will meet the requirements of section 15 of the NSR through the following proposed features:

- location and function
- design and construction
- measures to control access
- security equipment
- staffing

Onsite communications equipment, systems and procedures

The type and specifications of the proposed onsite communications equipment and systems that nuclear security officers will use to communicate with one another and with the security monitoring room during the activity to be licensed should be provided. Arrangements for maintaining the operation of non-portable communications equipment during a power outage should be included.

The procedures that nuclear security officers will follow to communicate with one another and with the security monitoring room during the activity to be licensed should be described. Means of secure communication for nuclear response forces should be provided, including secure radio communications and secure backup communications.

Offsite communications equipment, systems and procedures

The type and specifications of proposed offsite communications equipment and systems that nuclear security officers will use to communicate with offsite agencies, including those in the security monitoring room, should be described. The description should include proposed arrangements for maintaining the operation of non-portable communications equipment during a power outage.

The procedures and arrangements that nuclear security officers, including those in the security monitoring room, will follow to communicate with offsite agencies should be provided.

To ensure the reliability of communication devices implemented between on-site and off-site responses during the activity to be licenced, particular attention should be given to communication with emergency services, such as offsite armed-response forces.

6.2.5 Security systems, technical devices and equipment

Design and performance characteristics

In accordance with paragraph 3(c) of the NSR, the proposed security equipment, systems and procedures should be described, including:

- the purpose, function, design and performance of all security-related technical devices and their associated systems
- the detailed specifications of all security-related technical devices (such as the data supplied by the device manufacturers)
- a block diagram showing how the security systems integrate
- the operating procedures for all security-related technical devices
- the operating procedures for each security system

Maintenance, testing and inspection programs

The security program description should provide a description of the proposed maintenance, testing and inspection programs for the security systems, technical devices and equipment to be provided, in accordance with the requirements of paragraph 12(1)(d) of the GNSCR, including for the proposed:

- intrusion alarms
- detection devices
- emergency exit alarms
- lighting devices
- communications equipment

The proposed procedures, including schedules, for performing repairs and maintenance on the security system, technical devices and equipment during the activity to be licensed should be described. For scheduled maintenance activities, the security program description should provide:

- a listing of the security systems, technical devices and equipment to be maintained
- a brief description of the work to be performed
- a listing of the proposed service providers
- a description of the proposed service schedule

The proposed preventive maintenance program of security systems, subsystems and components should be described, including the corrective actions or compensating measures to be implemented in the event of failure of an essential component of the security system. The proposed program for the testing and inspection of security systems, technical devices and equipment during routine operation should be described, including the program's purpose, frequency and required thoroughness.

Equipment service manuals should not be included in the security program description.

6.3 Administrative security measures

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

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

- security organization
- contingency plans and procedures
- duties of nuclear security officers
- response to sabotage
- protection arrangements
- security awareness
- supervisory awareness program
- fitness for duty program

6.3.1 Security organization

Security roles within the facility organization

The proposed duties and responsibilities of executive and facility management who are responsible for overseeing the security program should be described. This includes all associated decisions during the activity to be licensed. A proposed single, designated point of contact for communication with the CNSC on physical security matters should be provided.

Structure and organization of the nuclear security officer service

The security program description should set out, in accordance with paragraph 3(e) of the NSR, the proposed structure and organization of the nuclear security officer service, including:

- the duties and responsibilities of the nuclear security officers
- the levels of authority and accountability of the security officer and nuclear response force members
- an organization chart of the proposed or actual facility that shows the reporting relationships between management and nuclear security officers
- the size of the security force, the number and scheduling of security shifts, the minimum complement of security officers for each shift, and the number and location of security posts for all shifts

Selection criteria for nuclear security officers

The criteria and procedures for recruiting, screening and appointing new nuclear security officers should be described.

Training of nuclear security officers and nuclear response force members

The proposed plan for training for nuclear security officers should be provided in accordance with section 34 of the NSR, including the course content, hours of training per subject, and testing methodologies for orientation training and follow-up “refresher” training, respectively.

Fitness of nuclear security officers

The security program description should provide a description of the proposed plan for fitness testing for nuclear security officers, in accordance with regulatory document RD-363, *Nuclear Security Officer Medical, Physical, and Psychological Fitness,* including the frequency of the testing, the certificate process and record retention, and a description of what is deemed a special circumstance.

Drills

Under subsection 36(4) of the NSR, the licensee should conduct security drills at least once a month to test the operation of the security equipment, systems and procedures at a nuclear facility consisting of a nuclear reactor that may exceed 10 MW thermal power during normal operation. The security program description should provide details on:

- how and when such drills will be conducted
- how the effectiveness of the drills will be evaluated

- how the results of a drill will be taken into account in subsequent drills

Equipment and vehicles for nuclear security officers and nuclear response force members

A description of the proposed number and specifications, and the conditions for use, of the equipment and vehicles to be provided to nuclear security officers should be provided, including any vehicle-related equipment, portable communications devices, night-vision aids, physical and radiation protection equipment, weapons or search devices.

Records

The proposed system and procedures for keeping, retaining and making available records in accordance with section 37 of the NSR, should be provided in the security program description, including those to be used to record:

- the name of each person to whom an authorization to enter a protected or inner area has been issued
- the duties and responsibilities of nuclear security officers
- the training received by each nuclear security officer
- the security procedures
- the reporting of security events
- the monitoring of the performance of nuclear security officers

Prescribed information

Measures to control access to prescribed information, as defined in section 21 of the GNSCR, and to prevent loss or illegal use, possession or removal of such prescribed information, should be proposed in the security program description.

6.3.2 Contingency plans and procedures

The proposed plan and procedures to assess and respond to breaches of security, in accordance with paragraph 3(f) of the NSR, should be provided, including information on proposed:

- methods to be used to assess a breach of security during the activity to be licensed
- responses to security incidents, such as intrusions, threats, theft of nuclear material, sabotage or civil disturbance, during the activity to be licensed
- procedures for responding to potential or actual breaches of security during the activity to be licensed
- command structure of the security force that will respond to breaches of security during the activity to be licensed
- procedures for transferring responsibility or command to an offsite force that is to respond to any breach of security during the activity to be licensed

Any other contingency plan that may require the involvement of the proposed security force should be provided.

6.3.3 Availability and duties of nuclear security officers and nuclear response force members

The nuclear security description should include:

- the times when and the circumstances under which nuclear security officers are to be on call or on duty
- the proposed method for calling in additional nuclear security officers
- the proposed duties of nuclear security officers during emergency and non-emergency situations

6.3.4 Sabotage or attempted sabotage

Site

In accordance with paragraph 12(1)(h) of the GNSCR, the proposed measures to alert the licensee to acts of sabotage or attempted sabotage anywhere at the site of the licensed activity should be provided.

Nuclear facility

For a licence to operate a Class I nuclear facility consisting of a nuclear reactor that may exceed 10 MW thermal power during normal operation, a description in accordance with paragraph 6(l) of the *Class I Nuclear Facilities Regulations* of the proposed measures to prevent acts of sabotage or attempted sabotage at the nuclear facility should be provided, including measures to alert the licensee to such acts.

6.3.5 Protection arrangements with offsite response forces

The nuclear security description should include a copy, in accordance with paragraph 3(a) of the NSR, of the proposed protection arrangements – such as detailed in a memorandum of understanding or some other document of commitment – made with an offsite response force pursuant to section 35 of the same regulations. The arrangements are signed and dated, in the presence of an attesting witness, by the applicant or the applicant's delegated representative, as well as by a delegated representative of the offsite response force.

A description of how the proposed protection arrangements will address section 35 of the NSR should be provided, including:

- estimates of the strengths of the proposed offsite response forces that are to be applied for situations ranging from an initial response to full activation of a response team
- estimates of the lengths of time required to deliver various levels ("initial" to "full") of planned responses
- the assessment, in consultation with the proposed offsite response force, of the types of security threats that the response force will be capable of handling with respect to the activity or facility to be licensed
- a description of the proposed offsite response force's arrangements for requesting and receiving support from another response force such as a police force

6.3.6 Security awareness

The proposed measures to instruct, in accordance with paragraph 12(1)(j) of the GNSCR, workers – employees, contractors and others – on the physical security program at the site of the licensed activity and on their obligations under that program, should be provided. Workers should be made aware of the following:

- the legal requirement for a person to immediately report to the nearest nuclear security officer, anyone who is not authorized to be in an area, pursuant to subsection 24(2) of the NSR
- the legal obligations of workers as per section 17 of the GNSCR

6.3.7 Supervisory awareness program

The proposed measures to develop and implement on an ongoing basis and maintain an effective supervisory awareness program to ensure that licensees' supervisors are trained to recognize behavioural changes in all personnel, including contractors, that could pose a risk to security at a facility at which it carries on licensed activities. The descriptions should also include the criteria used to demonstrate the effectiveness of the supervisory awareness program.

7. Transport Security Measures

This section provides guidance that applicants for a licence to transport Category I, II or III nuclear material may use when developing a transportation security plan under section 5 of the Nuclear Security Regulations (NSR). The following measures derive from regulatory requirements, national practices and international arrangements, and apply to all or specific categories of nuclear material, as indicated by the respective headings.

7.1 Measures for all categories of nuclear material

7.1.1 International protocols

Canada is a party to the *Convention on the Physical Protection of Nuclear Material (2005 Amendment)*, developed under the auspices of the International Atomic Energy Agency (IAEA). The convention calls upon parties to cooperate in providing protection of nuclear material during its transport across national borders. Parties are to apply protocols in concurrence with IAEA Nuclear Security Series No. 13 – *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5).

Before nuclear material is transported internationally, the shipper should ensure that the transport arrangements are in accordance with the physical protection regulations of the receiving country, and of any other countries through which the shipment is to pass. The nuclear regulatory agencies in the countries involved should be aware of the planned transport of nuclear material across a national border, and should be in agreement as to who will be responsible for the shipment at the various stages. The shipper and the receiver of the nuclear material that is to be transported across a national border should have an agreement that clearly states the point at which the responsibility for physical protection of the shipment transfers from the shipper to the receiver.

As long as material is within the borders of a country, it is subject to the regulatory regime of that country. For example, in the case of shipments between Canada and the United States, responsibility for physical protection begins and ends at the border between the two countries. This means that a shipment entering Canada from the United States becomes the responsibility of the CNSC licensee as soon as it enters Canada. Accordingly, if the nuclear material is to be imported into Canada, or exported from Canada, the receiver, or the shipper, respectively, must obtain from the CNSC, before the shipment crosses the border, the appropriate transport licence, along with an import licence in the former case, and an export licence in the latter.

Where a shipment of nuclear material might pass through the territory, including the territorial waters and airspace, of more than two countries, the sending and receiving countries should

include the other countries in their arrangements in order to enlist their cooperation in assuring adequate physical protection of the shipment.

7.1.2 Other principles

Since nuclear material can be especially vulnerable to theft or acts of sabotage when being transported, licensees should provide to nuclear material that is in transport a level of physical protection comparable to that provided for similar material during use or storage.

The total time that the nuclear material remains in transport should be minimized. The number and duration of any transfers of the nuclear material from one conveyance vehicle to another, or to and from temporary or longer-term storage, should also be minimized.

Fixed transport schedules for the movement of the nuclear material should be avoided. The routes used to transport the nuclear material should be varied, taking into account applicable regulations and ordinances regarding transport routes for radioactive and hazardous materials. Data about the movement of the nuclear material should be restricted to authorized persons.

Preliminary arrangements for the shipment of the nuclear material should be made with the receiver before the material is shipped, and details such as mode of transport, the handover point and the arrival time should be subsequently confirmed.

The trustworthiness of everyone who is to be involved in the transport of the nuclear material should be verified in advance of shipment, in accordance with the licensee's established procedures.

Where warranted, a transport security control centre (or security monitoring room (SMR), where applicable) should be established to coordinate the transport of the nuclear material and to make sure that secure and reliable communications are in place at all times during the transport of the nuclear material.

7.2 Category-specific measures

7.2.1 Measures for the transport of Category I nuclear material

Escorts

Shipments of Category I nuclear material should be accompanied by armed guards, or continuously escorted by a vehicle containing armed guards. The guards should maintain routine communications with the shipper, the receiver, the local authorities and the response forces along the transport route, until such time as responsibility for the shipment has been transferred to the receiver.

Communications

The shipper of Category I nuclear material should, in advance of the planned shipment, inform the receiver of the characteristics of the nuclear material, its planned modes of transport, and its anticipated date, time and location of arrival.

Before the transport begins, the shipper should confirm that the receiver is willing and prepared to receive the shipment. Upon the arrival of the shipment, the receiver should immediately notify the shipper. If the shipment does not arrive at its intended destination after an interval agreed to in

advance by the shipper and the receiver, the receiver should immediately notify the shipper of the incident.

Reliable and secure communications are essential during the transport of Category I nuclear material. Communications by two-way radio concerning the transport of such nuclear material should consist of encrypted messages only. During the transport, the escort should remain in frequent contact with the shipper, the receiver, the local authorities and the response forces along the transport route. When planning for the shipment, the shipper should establish a plan of action in the event that communications are lost during shipment. The establishment of a transport security control centre (or SMR, where applicable) should be considered.

If a shipment of nuclear material is lost or stolen, the licensee must, pursuant to paragraph 27(b) of the NSCA and paragraph 29(1)(a) of the *General Nuclear Safety and Control Regulations* (GNSCR), immediately make a preliminary report to the CNSC of the location and circumstances of the situation and of any action that the licensee has taken or proposes to take with respect to the situation.

Locks and seals

Packages that contain Category I nuclear material should be transported in closed, locked and sealed vehicles or freight containers. Where necessary, packages that contain Category I nuclear material and weigh more than 2,000 kg may, if locked, sealed and secured to the vehicle or freight container, be transported on an open vehicle. The integrity of the package locks and seals should be checked before departure, during the journey and on arrival at the final destination, in order to detect, in a timely manner, any tampering.

Security measures

All shipments of Category I nuclear material should be made, regardless of the mode of transport, in vehicles that are dedicated solely to the transport of such material.

Before shipping the nuclear material, the shipper should ensure that the selected carrier is aware of, and can comply with, the required physical security measures. When dealing with third-party carriers, the shipper should emphasize to the carrier the need for confidentiality in matters concerning shipments of Category I nuclear material and the need for the carrier to assure that everyone under the carrier's control who is to be involved in the planned transport of nuclear material is trustworthy.

Before a vehicle is loaded with a shipment of Category I nuclear material, appropriately trained personnel should conduct a rigorous search of the vehicle to ensure that there has been no attempt to sabotage it. Immediately following completion of the security search of the vehicle, it should be closed, locked, sealed and placed in a secure area pending its loading for transport.

Transport by road

Any vehicle that is to be used to transport Category I nuclear material by road should be manned and loaded so as to deter sabotage or theft of the cargo during transport. The driver of the transport vehicle should be accompanied by an armed guard, and the transport vehicle itself should be escorted by a separate vehicle carrying a driver and one or more armed guards. The escort vehicle should maintain constant surveillance of the shipment. The cargo should be firmly secured to the transport vehicle.

Transport by rail

During transport by rail, Category I nuclear material should be carried in a freight car of a railway train dedicated to the transport of freight. The car should be locked and sealed. Two or more guards should maintain constant surveillance of the car containing the nuclear material by travelling in an adjoining car. At regular intervals, the guards should check the integrity of the locks and seals of the freight car.

Transport by ship

During transport by ship, Category I nuclear material should be carried in a locked and sealed freight container that is securely loaded onto a vessel dedicated to the transport of cargo. Two or more guards should accompany the shipment and maintain constant surveillance of it. At regular intervals, the guards should check the integrity of the locks and seals of the freight container.

Transport by air

During transport by air, Category I nuclear material should be carried in a locked and sealed freight container that is placed on a chartered aircraft dedicated to the transport of cargo. Two or more guards should accompany the shipment and maintain constant surveillance of it. At regular intervals, the guards should check the integrity of the locks and seals of the freight container.

7.2.2 Measures for the transport of Category II nuclear materials

Escorts

Shipments of Category II nuclear material should be accompanied by one or more escorts, such as nuclear security guards authorized pursuant to section 18(2) of the NSR. These escorts should maintain constant surveillance of the shipment by travelling in the cargo vehicle or in an accompanying vehicle.

Communications

The shipper of Category II nuclear material should, in advance of the planned shipment, inform the receiver of the characteristics of the nuclear material, its planned modes of transport, and its anticipated date, time and location of arrival.

Before the transport begins, the shipper should confirm that the receiver is willing and prepared to receive the shipment. Upon the arrival of the shipment, the receiver should immediately notify the shipper of the arrival. If the shipment does not arrive at its intended destination after an interval agreed to in advance by the shipper and the receiver, the receiver should immediately notify the shipper of the incident.

During the transport of Category II nuclear material, the escort should remain in frequent contact with the shipper, the receiver, the local authorities and the response forces along the transport route. When planning for the shipment, the shipper should establish a plan of action in the event that communications are lost during shipment. The establishment of a transport security control centre (or SMR, where applicable) should be considered.

If a shipment of nuclear material is lost or stolen, the licensee must, pursuant to paragraph 27(b) of the *Nuclear Safety and Control Act* and paragraph 29(1)(a) of the GNSCR, immediately make

a preliminary report to the CNSC of the location and circumstances of the situation and of any action that the licensee has taken or proposes to take with respect to the situation.

Locks and seals

Packages that contain Category II nuclear material should be transported in closed, locked and sealed vehicles or freight containers. Where necessary, packages that contain Category II nuclear material and weigh more than 2,000 kg may, if locked, sealed and secured to the vehicle or freight container, be transported on an open vehicle. The integrity of the package locks and seals should be checked before departure, during the journey and on arrival at the final destination, in order to detect, in a timely manner, any tampering.

Security measures

Before shipping Category II nuclear material, the shipper should ensure that the selected carrier is aware of, and can comply with, the required physical security measures. When dealing with third-party carriers, the shipper should emphasize to the carrier the need for confidentiality in matters concerning the shipments of Category II nuclear material and the need for the carrier to assure that everyone under the carrier's control who is to be involved in the planned transport of nuclear material is trustworthy.

The number of cargo transfers during the shipment of Category II nuclear material and the length of time the shipment is in active transport, should be minimized.

Transport by road

Before a vehicle is loaded with a shipment of Category II nuclear material, qualified personnel should conduct a rigorous security search of the vehicle to ensure that there has been no attempt to sabotage it. Immediately following completion of the security search of the vehicle, it should be placed in a secure area pending its loading for transport. The transport vehicle, once loaded with Category II material for transport and in transit, should be locked and sealed when not on the move, and should never be left unattended.

Transport by rail

During transport by rail, Category II nuclear material should be carried in a car of a train dedicated to the transport of freight, or in a dedicated freight car attached to a passenger train. The car should be locked and sealed.

Transport by ship

During transport by ship, Category II nuclear material should be carried in a locked and sealed freight container.

Transport by air

During transport by air, Category II nuclear material should be carried in a locked and sealed freight container that is placed on an aircraft dedicated to the transport of cargo.

7.2.3 Measures for the transport of Category III nuclear material

Communications

The shipper of Category III nuclear material should, in advance of the planned shipment, inform the receiver of the characteristics of the nuclear material, its planned modes of transport, and its anticipated date, time and location of arrival.

Before the transport begins, the shipper should confirm that the receiver is willing and prepared to receive the shipment. Upon the arrival of the shipment, the receiver should immediately notify the shipper of the arrival. If the shipment does not arrive at its intended destination after an interval agreed to in advance by the shipper and the receiver, the receiver should immediately notify the shipper of the incident.

If a shipment of nuclear material is lost or stolen, the licensee must, pursuant to paragraph 27(b) of the NSCA and paragraph 29(1)(a) of the GNSCR, immediately make a preliminary report to the CNSC of the location and circumstances of the situation and of any action that the licensee has taken or proposes to take with respect to the situation.

Locks and seals

Packages that contain Category III nuclear material should be transported in closed, locked and sealed vehicles, or in locked and sealed freight containers, when feasible.

Security measures

Before shipping Category III nuclear material, the shipper should ensure that the selected carrier is aware of, and can comply with, the required physical security measures. When dealing with third-party carriers, the shipper should emphasize to the carrier the need for confidentiality in matters concerning the shipments of Category III nuclear material and the need for the carrier to assure that everyone under the carrier's control who is to be involved in the planned transport of nuclear material is trustworthy.

The number of cargo transfers during the shipment of Category III nuclear material and the length of time the shipment is in active transport, should be minimized.

Transport by road

Before a vehicle is loaded with a shipment of Category III nuclear material, qualified personnel should conduct a rigorous security search of the vehicle to ensure that there has been no attempt to sabotage it. Immediately following completion of the security search of the vehicle, it should be placed in a secure area pending its loading for transport. The transport vehicle, once loaded with Category III material for transport and in transit, should be locked and sealed when not on the move, and should never be left unattended.

Transport be rail

During transport by rail, Category III nuclear material should be carried in a car of a train dedicated to the transport of freight, or in a dedicated freight car attached to a passenger train. The car should be locked and sealed.

Transport by ship

During transport by ship, Category III nuclear material should be carried in a locked and sealed freight container.

Transport by air

During transport by air, Category III nuclear material should be carried in a locked and sealed freight container that is placed on an aircraft dedicated to the transport of cargo.

8. Transportation Security Plan

8.1 Content

To comply with section 5 of the NSR, an application for a licence to transport Category I, II or III nuclear material shall include a written transportation security plan that contains the information required by paragraphs 5(a) to (h) of the same regulations. Guidance on the information that is to be included in the plan to meet these requirements is provided below. In addition, section 7 of this document recommends measures on protecting nuclear material during transport that the applicant may find useful when developing a transportation security plan.

Guidance

The primary purpose of a transportation security plan is to assure that the nuclear material to be transported will receive adequate physical protection against any threats that may arise during its transport. Accordingly, the security measures provided for in the proposed plan should be commensurate with the category of the nuclear material that is to be transported, and with the associated threats. That is, security measures for the transport of Category I nuclear material should typically be more stringent than for the transport of Category II nuclear material, and those for the transport of Category II nuclear material more stringent than for Category III nuclear material.

When applying for a licence to transport Category I, II or III nuclear material, the applicant can expedite CNSC review and processing of the application by submitting a security transportation plan that follows appendix D of this document and that adopts the subject headings of sections 8.1.1 to 8.1.8.

Throughout the plan, applicants should, whenever possible, name the key persons involved, provide their position titles, and describe their associated roles, responsibilities, authorities and accountabilities.

8.1.1 Administrative information

The administrative information should include:

- the complete legal name and business address of the applicant who is submitting the plan in support of a licence application pursuant to section 5 of the NSR
- the complete legal name and business address of any individual who is authorized to serve as the applicant's representative in discussions with the CNSC concerning matters pertaining to the plan

- the telephone and fax numbers, or email addresses at which the applicant, or any representative of the applicant in matters pertaining to the plan, may be contacted during normal business hours
- a description of the licence application to which the plan pertains

8.1.2 Description of the nuclear material

Pursuant to paragraph 5(a) of the NSR, the description of the nuclear material to be transported should include:

- the name of the nuclear material
- the category and quantity of the nuclear material (gross mass, net mass and mass of nuclear material)
- the chemical and physical characteristics of the nuclear material
- the isotopic composition of the nuclear material
- the degree of enrichment or dilution of uranium 235, uranium 233 or plutonium
- the radiation level, in Gy/h, of the overall shipment as well as that of its discrete parts

8.1.3 Threat assessment

Pursuant to paragraph 5(b) of the NSR, a transportation security plan shall include "a threat assessment consisting of an evaluation of the nature, likelihood and consequences of acts or events that may place prescribed information or nuclear material at risk".

Guidance

All credible threats to the security of the shipment should be identified. Threat assessments for Category I and II shipments should be considerably more thorough than those for Category III shipments.

The CNSC expects that applicants, when evaluating threats to a proposed transport of Category I, II or III nuclear material, will communicate with their appropriate law enforcement agencies to determine whether these agencies consider the threats to be high, medium or low, and will factor the response received into the overall assessment.

The CNSC receives, from the responsible federal security agencies, assessments that identify known criminal, extremist or terrorist threats that involve the movement of nuclear material. Thus, the applicant, when preparing the application for a licence to transport Category I, II or III nuclear material, should contact the CNSC to determine whether it is aware of any special information that should be taken into account in the applicant's threat assessment.

8.1.4 Description of the conveyance

Paragraph 5(c) of the NSR requires that the transportation security plan provide "a description of the conveyance" for the proposed transport. This description should cover the act of conveyance from the time the shipment leaves its originating location until it reaches its planned destination. It should describe how the nuclear material will be contained or secured for transport, including the type, design, size and weight of any container to be used and any provision for securing the container to the transport vehicle.

If the proposed conveyance involves more than one mode of transport and multiple transfers of the nuclear material – for example, by road to a rail terminal, followed by rail transport for a

further stage of the journey, and finally by road to the planned destination site – the details of the conveyance should be provided for each segment of the journey. These details should include the date, time and location of the planned transfers and the names of the persons to be responsible for ensuring the success of the transfers, and for verifying the integrity of the associated shipments.

Where interim storage of the nuclear material may be required during conveyance, the proposed security measures for the conveyance should provide for safe interim storage of the materials, as discussed in section 8.1.5.

Where interim storage of the nuclear material may be required during conveyance, the proposed security measures for the conveyance should provide for secure interim storage of both the vehicle and materials, as discussed in section 8.1.5.

8.1.5 Proposed security measures

As required by paragraph 5(d) of the NSR, a description of the proposed security measures must be included in the transportation security plan.

Guidance

To provide adequate protection during a conveyance, the proposed security measures should be commensurate with the specific circumstances. These measures should take into account the category of nuclear material to be transported, the size and type of the shipment, the distance and type of terrain to be covered, the mode of transport, the results of the threat assessment, and public concerns. Accordingly, the proposed security measures should typically describe:

- whether the shipment of Category I, II or III nuclear material is to be sealed or unsealed
- whether armed or unarmed guards, escort personnel or escort vehicles are to be utilized
- the number of any armed or unarmed guards, escort personnel or escort vehicles to be utilized
- any provisions for the support of response forces along the transport route
- any procedures for contacting, during the act of conveyance, the response force from any involved jurisdiction or agency
- provisions for rigorous security searches of the proposed conveyance vehicles prior to shipment of nuclear material, for the purpose of detecting any sabotage attempt or other threat
- contingency arrangements to address such events as a mechanical breakdown of a transport or escort vehicle, or a failure of the shipment to arrive at its destination at the expected time
- the procedures to be followed during any scheduled stop, or unscheduled delay, during transport
- the measures to be in place at Canadian ports, air cargo terminals or other locations where the nuclear material is to be stored and secured during transport

The level of security for nuclear materials during interim storage while in transport, including during each overnight stop, should typically be comparable to that provided for the same category of nuclear material during its storage at a licensed nuclear facility. These security arrangements should take into account the location of the proposed interim storage and the nuclear material's potential appeal to thieves or terrorists.

When proposing to transport nuclear materials on journeys that could take more than one day, the applicant should include provision for overnight stays at a prearranged location where the transport vehicle carrying the nuclear material can be immobilized and kept in a physically secure

and appropriately monitored area. The provisions for preventing theft of the nuclear materials should include securing the materials to the vehicle.

In addition to dealing with scheduled stops at prearranged locations, the transportation security plan should describe the security measures to be taken in the event of unexpected delays caused by natural or other hazards.

The applicant should attempt to anticipate and address, at an early stage, any special public concerns regarding the proposed transport that could lead to negative media coverage and to protests or demonstrations. Accordingly, the applicant should provide for effective contacts with local and provincial response forces in order to gain early notice of any road closures or detours implemented to deal with such incidents.

8.1.6 Communication arrangements

Paragraph 5(e) of the NSR requires that the communication arrangements that will be in place throughout the transport of the nuclear material be part of the transportation security plan. These may include communication arrangements with:

- the licensee
- the operator of the vehicle transporting the nuclear material
- the recipient of the material
- any response force along the transport route
- any transport security control centre (or security monitoring room (SMR), where applicable) that is to be established for the operation

If the licence applicant proposes to use cellular phones for communications during the transport of Category II or III nuclear material, the proposal should provide for limited use of such phones and encryption of messages where possible. It is important that all those involved in the transport and security of nuclear material be aware that unencrypted communications by cellular phone are not secure. Accordingly, the use of cellular phones to send unencrypted messages regarding the transport of Category I nuclear material is not recommended. For such situations, radio systems that utilize encryption features provide a more secure means of communication.

Whether a radio or a cellular phone is to be used, it is important to assure that communications coverage is adequate along the entire route. In remote regions, there may be gaps in cellular or radio coverage. Where it may not be possible to avoid such “blackout” areas along the transport route, other communications arrangements should be proposed. Satellite and global positioning systems (GPS) provide for continuous tracking and monitoring in areas where cellular coverage is limited or unavailable.

For each primary communication method proposed, the transportation security plan should include appropriate emergency backup provisions. For example, where the use of cellular phones is proposed, the applicant should provide for the supply of more than one phone and supplementary power sources for the phones.

Applicants who plan to make regular shipments of nuclear material may wish to propose the establishment of a transport security control centre. Typically, such a centre would be operated during the shipment of nuclear material. Where the applicant proposes to establish a transport security control centre, the proposal should include provision for the training of the persons who will staff the centre. These staff should be trained in the techniques to be used to monitor the

proposed shipments of nuclear materials, and in the proposed communications arrangements among the parties listed above.

The transportation security plan should also indicate the action to be taken if communications contact with a vehicle carrying nuclear material is lost. For such situations, applicants may wish to consider the use of electronic and satellite tracking devices, such as transponders that can be concealed on a vehicle or in the shipment. Such devices could be used to track the vehicle carrying nuclear material, and could be particularly useful in situations where communications are interrupted.

The proposed communications arrangements with response forces along the transport route should include notifying the relevant response force of any scheduled or unscheduled overnight stops, including the exact location of the overnight stops.

8.1.7 Arrangements with response forces

In accordance with paragraph 5(f) of the NSR, the transportation security plan must include the arrangements to be made between the licensee and any response force along the transport route.

Guidance

The applicant's proposed arrangements should include provisions for establishing effective communications with any response force along the transport route, in accordance with section 8.1.6 above. The provisions should include notifying the response force from any involved jurisdiction or agency of the shipment, in advance of the actual transport.

As part of the applicant's proposed arrangements, a response force, such as a local law enforcement agency or a private security firm, may provide an armed escort for a shipment of nuclear material. Where the arrangements involve more than one law enforcement agency, the plan should describe the cooperative arrangements for transferring responsibility from one response force to another. For example, a transport route that crosses the border between Quebec and an adjoining province would pass through the jurisdiction of the Sûreté du Québec, as well as the jurisdiction of the Ontario Provincial Police or the Royal Canadian Mounted Police and, where these respective forces serve as escorts, would require corresponding transfers of responsibility. Accordingly, all changes in the proposed communications methods or protocols for the planned transfers of responsibility along a transport route – such as changes in radio frequencies or radio or cellular encryption methods – should be clearly described in the plan.

8.1.8 Planned and alternate routes

Under paragraphs 5(g) and (h) of the NSR, the transportation security plan shall include descriptions of "the planned route" and "the alternate route to be used in the event of an emergency".

Guidance

When selecting the planned or alternate routes for the transport of nuclear material, the applicant should take into account applicable regulations and ordinances regarding transport routes for hazardous materials, and choose routes that bypass urban areas wherever practical. However, if the proposed route is to pass through an urban area, the applicant should describe the precise route to be taken through the area and how the shipment is to be scheduled to avoid times of peak traffic.

When proposing an alternate route, the applicant should take into consideration the feasibility and logistics of switching from one route to another during the transport of nuclear materials. For example, to facilitate potential switches from a planned route to an alternate route, and vice versa, the applicant should ensure that adequate transportation connections exist between the proposed routes, and should provide accurate descriptions of the proposed routes for transferring between the planned and alternate routes.

When choosing routes for the transport of nuclear material, the applicant should take into account any obvious hazards, such as rockslides, floods or forest fires, that could adversely affect the transport at certain times.

8.2 Confidentiality

Since a transportation security plan for a licence to transport Category I, II or III nuclear material contains "prescribed information" for the purposes of the NSCA, it must be handled in such a way as to protect such information in accordance with the applicable provisions of the GNSCR. Licence applicants and licensees must take all necessary precautions to prevent unauthorized access to any prescribed information contained in a transportation security plan. Accordingly, the CNSC recommends that the licensees follow appendix D when preparing, submitting or revising a transportation security plan.

8.3 Regulatory review and licensing

After receiving an application for a licence to transport Category I, II or III nuclear material with the transportation security plan, the CNSC will evaluate the adequacy of the information submitted and will accordingly:

- if the application meets regulatory requirements, issue the requested licence at its earliest convenience, or as requested by the applicant
- if the application is incomplete or if the information provided is inadequate, advise the applicant of the deficiency

Where circumstances warrant, an applicant for any CNSC licence may choose to deliberately submit an incomplete application, requesting CNSC review of the same. In such cases, the applicant should provide justification for the request and a schedule for completing the application.

To allow maximum time for regulatory review and processing of applications for such a licence, the CNSC encourages the applicants to submit their proposed transportation security plans as soon as possible and in advance of the rest of the application where necessary in the interests of timeliness.

The transportation security plan is fundamental to the safety and security of the proposed transport and, accordingly, will be subjected to rigorous regulatory review. Where this review identifies deficiencies, the deficiencies will need to be resolved before the licence to transport Category I, II or III nuclear material may be issued.

Appendix D to this guide provides advice on preparing, submitting and revising transport security plans.

Appendix A: Sample Site Security Plan for Category 1, 2 or 3 Sealed Sources

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

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.

A1. 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

A2. 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

A3. Security policy

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

A4. 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

A5. 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

A6. 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

A7. 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

A8. 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

A9. Transportation

- provide a list of vehicles used for the transportation of 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

A10. 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

A11. 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

A12. 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)

A13. 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

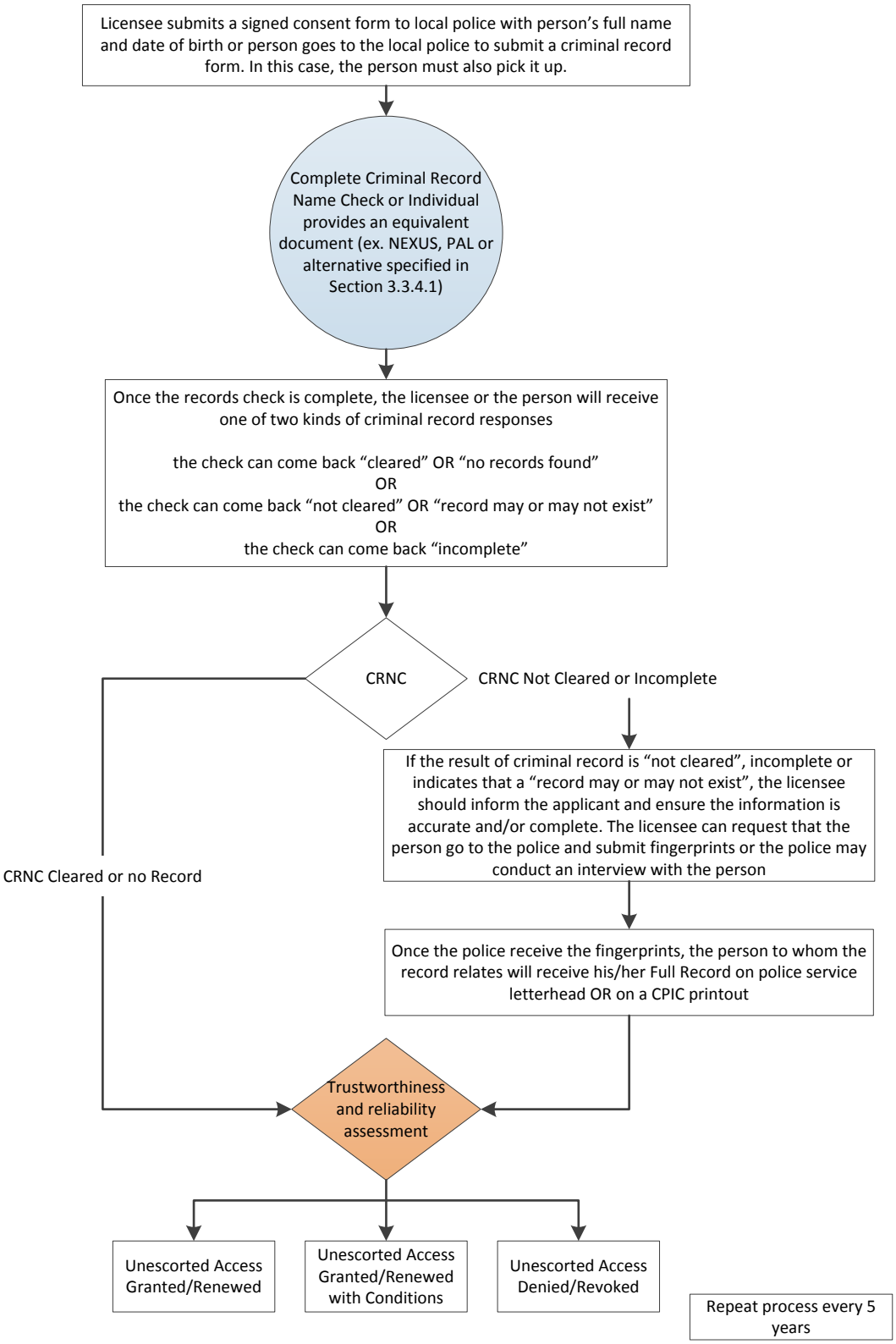
A14. Security awareness program

- 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)

A15. 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: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 3: Application of REGDOC-2.12.3, Part A, *Security of Sealed Sources* for typical uses of sealed sources

Appendix D: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 3: Application of REGDOC-2.12.3, Part A, *Security of 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 radiotherapy	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

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
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	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Thickness gauges	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Fill-level, thickness gauges	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Moisture detectors	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Density gauges	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Moisture/density gauges	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Static eliminators	4	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
X-ray fluorescence analyzers	5	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Electron capture detectors	5	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Brachytherapy low dose rate eye plaques and permanent implants	5	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P
Positron Emission Tomography (PET) checking	5	Y	Y	Y	P	P	P	P	P	P	P	Y	Y	P	P	P	P

Appendix E: Preparing, Submitting and Revising the Security Program Description or Transport Security Plan

This appendix provides recommendations to help applicants and licensees prepare and submit, or revise the security program description that consolidates the security information that is to be included in an application for a licence – other than a licence to transport – in respect of:

- Category I or II nuclear material
- a nuclear facility consisting of a nuclear reactor that may exceed 10 MW thermal power during normal operation

This appendix also provides recommendations to help applicants and licensees prepare and submit, or revise, a transportation security plan for Category I, II, or III nuclear material.

For the purposes of this appendix, the term "document" refers to either the security program description or a transportation security plan.

E.1 General

The information contained in the security program description or transportation security plan should be clear and concise. Definitions and abbreviations used should be consistent throughout the document. The specialized terms used should conform to those defined or used for comparable purposes in relevant regulations. Any drawing or sketch included in the document should be large enough so as to be clearly legible.

To minimize duplication, information that is provided in one section of the document may be cross-referenced for the purposes of other sections of the document.

E.2 Confidentiality and security

Pursuant to sections 21 and 23 of the *General Nuclear Safety and Control Regulations* (GNSCR), the security program description or security transportation plan is "prescribed information" and must be protected to prevent any unauthorized access. This requires that the document, and all correspondence between the Canadian Nuclear Safety Commission (CNSC) and licence applicants or licensees that concerns the document, be treated as confidential or protected information, as follows:

- The top right-hand corner of each page of the document should bear the security classification level of the document, that is, "**CONFIDENTIAL — PRESCRIBED INFORMATION**", in bold, uppercase letters.
- The document and the related correspondence may be forwarded to the CNSC by mail or courier.

For delivery to the CNSC, the document and the related correspondence should be "double-enveloped", with the document and correspondence contained within the inner envelope or package. The inner envelope or package should be addressed to the "Director, CNSC Nuclear Security Division", sealed and clearly marked "CONFIDENTIAL–PRESCRIBED INFORMATION", labelled "TO BE OPENED BY THE ADDRESSEE ONLY", and inserted into an outer envelope or package. The outer envelope or package should be sealed and addressed to:

Canadian Nuclear Safety Commission
280 Slater Street

P. O. Box 1046, Station B
Ottawa, Ontario K1P 5S9

If the transportation security plan and the related correspondence are sent to the CNSC by "secure facsimile", the transmission should meet the Level I ("Confidential") requirements of the Communications Security Establishment.

Upon receiving the document or the related correspondence, the CNSC will protect it from unauthorized disclosure, in accordance with the GNSCR and the *Access to Information Act*.

E.3 Style, structure and layout

The document should include a title page, a table of contents and a glossary of any specialized terms used in the document. It should display a unique identifier. The pages should be numbered sequentially.

Information items should be numbered and identified, as appropriate, according to the sequence and headings given in section 6 of this regulatory document for a security program description or according to the sequence and headings given in subsection 8.1 of this regulatory document for a transportation security plan.

E.4 Revising the program or plan

CNSC licensees must comply with the applicable regulations and licence conditions, including any condition of their licence that requires them to adhere to a referenced security program description or transportation security plan. To modify the referenced document, the licensee must submit a revised version to obtain CNSC approval of the proposed changes.

When requesting CNSC approval to revise an existing security program description or transportation security plan, the licensee should identify, and explain the reasons for, the proposed changes. The request for approval should include a single, complete copy of the new version of the document. To assist CNSC review, the proposed revisions or revised sections should be underlined or highlighted. The proposed document should follow the above recommendations and be clearly identified, using the convention described in section D.3 above.

Appendix F: Category I, II and III Nuclear Material

Category I, II and III nuclear material are defined as follows in section 1 of the *Nuclear Security Regulations* (NSR), and in its Schedule 1.

- **Category I nuclear material** means "a nuclear substance listed in column 1 of the schedule [see below] that is in the corresponding form set out in column 2 and the corresponding quantity set out in column 3 of the schedule."
- **Category II nuclear material** means "a nuclear substance listed in column 1 of the schedule [see below] that is in the corresponding form set out in column 2 and the corresponding quantity set out in column 4 of the schedule."
- **Category III nuclear material** means "a nuclear substance listed in column 1 of the schedule [see below] that is in the corresponding form set out in column 2 and the corresponding quantity set out in column 5 of the schedule."

Nuclear substance	Form	Quantity (Category I)[1]	Quantity (Category II)[1]	Quantity (Category III)[1,2]
Plutonium[3]	Unirradiated[4]	2 kg or more	Less than 2 kg, but more than 500 g	500 g or less, but more than 15 g
Uranium 235	Unirradiated[4] – uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg, but more than 1 kg	1 kg or less, but more than 15 g
Uranium 235	Unirradiated[4] – uranium enriched to 10% ^{235}U or more, but less than 20% ^{235}U	N/A	10 kg or more	Less than 10 kg, but more than 1 kg
Uranium 235	Unirradiated[4] – uranium enriched above natural, but less than 10% ^{235}U	N/A	N/A	10 kg or more
Uranium 233	Unirradiated	2 kg or more	Less than 2 kg, but more than 500 g	500 g or less, but more than 15 g
Fuel consisting of depleted or natural uranium thorium or low-enriched fuel (less than 10%	Irradiated	N/A	More than 500g of plutonium	500 g or less, but more than 15 g of plutonium

Nuclear substance	Form	Quantity (Category I)[1]	Quantity (Category II)[1]	Quantity (Category III)[1,2]
fissile content)[5]				

Source: NSR, Schedule 1

1. The quantities listed refer to the aggregate of each kind of nuclear substance located at a facility, excluding the following (which are considered separate quantities):
   a. any quantities of the nuclear substance that is not within 1,000 m of another quantity of the nuclear substance
   b. any quantity of the nuclear substance that is located in a locked building or a structure offering similar resistance to unauthorized entry
2. Quantities less than the quantities set out in column 5 for Category III nuclear material and any quantities of natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent security practice.
3. All plutonium except that with isotopic concentration exceeding 80% in plutonium 238
4. Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h at 1 m unshielded
5. Other fuel that by virtue of its original fissile content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h at 1 m unshielded.

Glossary

For definitions of terms used in this document, see REGDOC-3.6, *Glossary of CNSC Terminology*, which includes terms and definitions used in the *Nuclear Safety and Control Act* and the regulations made under it, and in CNSC regulatory documents and other publications. REGDOC-3.6 is provided for reference and information.

access control
A system for allowing only approved individuals to have unescorted access to the security zone and for ensuring that all other individuals are subject to escorted access.

adversary
A person performing malevolent acts in pursuit of interests harmful to the facility; an adversary may be an insider or an outsider.

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

contingency plan
Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

encapsulated source
Radioactive material that is permanently sealed in a capsule or closely bounded in a solid form.

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**.**

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.

References

1. International Atomic Energy Agency (IAEA), *Code of Conduct on the Safety and Security of Radioactive Sources*, Vienna, 2004

2. IAEA, Safety Guide No. RS-G-1.9, *Categorization of Radioactive Sources*, Vienna, 2005

3. IAEA, TECDOC-1344, *Categorization of Radioactive Sources*, Revision of TECDOC-1191, Categorization of Radiation Sources, Vienna, 2003

4. IAEA, SSR-6, *Regulations for the Safe Transport of Radioactive Material*, 2012 edition

5. IAEA, TECDOC-1355, *Security of radioactive sources – Interim guidance for comment*, Vienna, 2003

6. ASTM F2548-06, *Standard Specification for Expanded Metal Fence Systems for Security Purposes*, ASTM International, West Conshohocken, PA, 2006

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

9. Treasury Board of Canada Secretariat, Government of Canada, *Policy on Government Security*, 2009

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

Additional Information

The following documents are not referenced in this regulatory document but contain information that may be useful to the reader:

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

2. 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

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

4. Canadian Nuclear Safety Commission (CNSC), REGDOC 2.12.1, *High-Security Sites: Nuclear Response Force*, Ottawa, Canada, 2013

5. CNSC, REGDOC-2.12.2, *Site Access Security Clearance*, Ottawa, 2013

6. CNSC, RD-321, *Criteria for Physical Protection Systems and Devices at High-Security Sites*, Ottawa, 2010

7. CNSC, RD-361, *Criteria for Explosive Substance Detection, X-ray Imaging, and Metal Detection Devices at High-Security Sites*, Ottawa, 2010

8. CNSC, RD-363, *Nuclear Security Officer Medical, Physical, and Psychological Fitness*, Ottawa, 2008

9. CSA Group, CSA N290.7-14, *Cyber security for nuclear power plants and small reactor facilities*, Toronto, 2014

10. International Atomic Energy Agency (IAEA), INFCIRC 274, Rev.1, *The Convention on the Physical Protection of Nuclear Material*, Vienna, 1980. Note: The CPPNM was amended in 2005 to include domestic nuclear material in use, process or storage. Canada has accepted this amendment but is awaiting formal IAEA ratification of same.

11. 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

12. IAEA, Nuclear Security Series No. 8, Implementing Guide, *Preventive and Protective Measures against Insider Threats*, Vienna, 2008

13. IAEA, Nuclear Security Series No. 9, Implementing Guide, *Security in the Transport of Radioactive Material*, Vienna, 2008

14. IAEA, Nuclear Security Series No. 10, Implementing Guide, *Development, Use and Maintenance of the Design Basis Threat*, Vienna, 2012

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

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

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

18. IAEA, Nuclear Security Series No. 15, Recommendations, *Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control,* Vienna, 2011

19. IAEA, Nuclear Security Series No. 16, Technical Guidance Reference Manual, *Identification of Vital Areas at Nuclear Facilities,* Vienna, 2012

20. IAEA, Nuclear Security Series No. 17, Technical Guidance Reference Manual, *Computer Security at Nuclear Facilities,* Vienna, 2011

21. IAEA, Nuclear Security Series No. 23-G, Implementing Guide, *Security of Nuclear Information*, Vienna, 2015

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 CNSC processes and practices
- 3.6 Glossary of CNSC terminology

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 website.