OPG Comments on RD/GD 338, "Security Measures for Sealed Sources"

Comment #	RD Document Section/ Excerpt of Section	OPG Issue or Comment	OPG Suggested Change
	Cover **Forward** **Preface**	No comment.	No change.
	1. Introduction 1.1 Purpose 1.2 Scope 1.3 Relevant Regulations 1.4 National and International Standards	No comment.	No change.
1	**2. Background**	Text Change.	Recommend changing Category1, 2, 3 to another scheme as use of this language may be confused with Category I, II, III nuclear mateial stored in high security areas.
	2.1 Application	No comment.	No change.
	2.2 Catergorization	No comment.	No change.
	2.2.1 Nuclear Substances and Thresholds for the Activity Levels	No comment.	No change.
	Table A: Activities Corresponding to Thresholds and of Category 1, 2 and 3 Sources	No comment.	No change.
	2.2.2 Methodology for Assigning a Category	No comment.	No change.

	3 Security Measures **3.1 General Security Measures** **3.1.1** **Requirements for general security measures** While in storage, licensees **shall** develop and implement technical and administrative security measures to protect the radioactive source against unauthorized removal (such as theft or loss) or sabotage. As outlined in IAEA TECDOC-1355 [4], 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.	No comment.	No change.
2	**3.1.2** **Guidance for general security measures** 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 the sealed source. The threat and risk assessment, updated annually, is also used to determine mitigating security measures to address identified threats, manage risks or reduce/eliminate vulnerabilities. Table B provides information on how security program subsections **should** be applied to Category 1 (high risk), Category 2 (high risk), Category 3 (medium risk), and Categories 4 and 5 (low risk).	Text Change.	Recommend annual TRA **review**, but actual update submission to CNSC is only when important changes are completed at the facility **or** if significant threat level change occurs.
	Table B Security Levels and Security Objectives **Category 1 High Risk** **Security Program Sub Sections**	**n/a - OPG does not possess Category 1 High Risk sources.** No comment.	No change.

	Facility Security Plan	• updated **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		
	Perimeter and Physical Barrier (1st Line of Defence)	• **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 Storage (2nd Line of Defence)	• secured with good quality padlock or equivalent security system		
		• equipped with a minimum of two intrusion detection **systems**		
		• secure containers **must** be able to resist an attack by handheld tools		
	Intrustion Detection System	• **must** 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		
	Access Control	• restrict access to authorized user only		
		• two-person rule (optimal)		
		• visitors, students, contractors **must** be escorted at all times		
	Transportation Security Plan	• **must** develop and submit a specific Transport Security Plan to CNSC for review and approval		
	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		
	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 (optimal)		
		• 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		
	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		
	Information Security	• all prescribed information **must** be protected and be shared on a need to know basis		
	Maintenance and Testing	• maintenance and testing **must** be conducted at least every six months, and written records **should** be maintained		

	Security Awareness Program	• all workers **must** receive security awareness training on a regular basis		
3	**Category 2 High Risk** **Security Program Sub Sections**			
	Facility Security Plan	• updated **annually** or when important changes are done at the facility	Text Change.	Recommend annual FPS **review**, but actual update submission to CNSC is only when important changes are completed at the facility.
		• classified prescribed and/or sensitive and stored appropriately	No comment.	No change.
		• communicated on a need to know basis	No comment.	No change.
		• indicate measures in case of increased threat	No comment.	No change.
	Perimeter and Physical Barrier (1st Line of Defence)	• **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	No comment.	No change.
	Security Storage (2nd Line of Defence)	• secured with good quality padlock or equivalent security system	No comment.	No change.

		• equipped with a minimum of two intrusion detection systems	Text Change.	OPG is of the opinion that two intrusion detection systems is excessive when one supervised intrusion detection system including two intrusion detection **devices** would provide the reliability and probabilty of detection required for sealed sources. Supervised systems also provide trouble alarms in the case of any fault that prompts response and compensatory measures. Recommend change of word 'systems' to devices.
		• secure containers **must** be able to resist an attack by handheld tools	No comment.	No change.
	Intrustion Detection System	• **must** 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	No comment.	No change.
	Access Control	• restrict access to authorized user only	No comment.	No change.
		• visitors, students, contractors **must** be escorted at all times	No comment.	No change.

	Transportation Security Plan	• **must** develop and maintain a generic Transportation Security Plan	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
	Response Protocol	• specific response protocol and contingency plan	No comment.	No change.
		• contact local law enforcement	No comment.	No change.
		• effective response time	No comment.	No change.
		• **must** develop a procedure in case of lost, stolen or malicious act involving radioactive sealed source	No comment.	No change.
	Vehicle Security	• vehicle **must** be equipped with anti-theft or vehicle disabler and intrusion detection system, or equivalent measures	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
		• 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 (optimal)		
		• 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		
	Personal Trustworthiness or Background Checks	• criminal records name check	No comment	No change.
		• reference, education and employment verification	No comment	No change.
		• drivers and contractors (i.e., carriers) with unescorted access to radioactive sources **must** undergo this verification	No comment	No change.
	Information Security	• all prescribed information **must** be protected and be shared on a need to know basis	No comment	No change.
	Maintenance and Testing	• maintenance and testing **must** be conducted at least every six months, and written records **should** be maintained	No comment	No change.
	Security Awareness Program	• all workers **must** receive security awareness training on a regular basis	No comment	No change.
5	**Category 3 Medium Risk** **Security Program Sub Sections**			
	Facility Security Plan	• updated on a **regular basis** or when important changes are done at the facility	Text Change.	Recommend regular FPS **review**, but actual update submission to CNSC is only when important changes are completed at the facility.
		• **must** be classified prescribed and/or sensitive and stored appropriately	No comment	No change.
		• communicated on a need to know basis	No comment	No change.

	Perimeter and Physical Barrier (1st Line of Defence)	• **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	No comment	No change.
	Security Storage (2nd Line of Defence)	• secured with good quality padlock or equivalent security system	No comment	No change.
6		• equipped with a minimum of one intrusion detection system	No comment	No change.
	Intrustion Detection System	• **must** 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	No comment	No change.
	Access Control	• restrict access to authorized user only	No comment	No change.
		• visitors, students, contractors **must** be escorted by authorized user	No comment	No change.
	Transportation Security Plan	• best practice	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
	Response Protocol	• generic response protocol and contingency plan	No comment	No change.
		• **must** develop a procedure in case of lost, stolen or malicious act involving radioactive sealed source	No comment	No change.

	Vehicle Security	• vehicle **must** be equipped with anti-theft and intrusion detection system or equivalent measures	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
		• vehicle **must** be equipped with a minimum of two technical barriers to prevent unauthorized removal	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
	Personal Trustworthiness or Background Checks	• Reference, education and employment verification	No comment	No change.
		• Criminal records name check	No comment	No change.
	Information Security	• all prescribed information **must** be protected and be shared on a need to know basis	No comment	No change.
	Maintenance and Testing	• maintenance and testing **must** be conducted at least every six months, and written records **should** be maintained	No comment	No change.
	Security Awareness Program	• all workers **must** receive security awareness training on a regular basis	No comment	No change.
	Category 4-5 Low Risk **Security Program Sub Sections**			
	Facility Security Plan	• best practice	No comment	No change.
	Perimeter and Physical Barrier (1st Line of Defence)	• source **must** be protected against unauthorized access and removal	No comment	No change.

	Security Storage (2nd Line of Defence)	• **must** be stored in a secure container or location	No comment	No change.
	Intrustion Detection System	• source **must** be protected against unauthorized access and removal	No comment	No change.
	Access Control	• source **must** be protected against unauthorized access and removal	No comment	No change.
	Transportation Security Plan	• source **must** be protected against unauthorized access and removal	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
	Response Protocol	• source **must** be protected against unauthorized access and removal	No comment	No change.
	Vehicle Security	• source **must** be protected against unauthorized access and removal	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A. Vendors would be responsible to meet this requirement.** No Comment.	No change.
	Personal Trustworthiness or Background Checks	• Reference, education and employment verification	No comment	No change.
		• Criminal records name check (best practice)	No comment	No change.
	Information Security	• all prescribed information **must** be protected and be shared on a need to know basis	No comment	No change.

	Maintenance and Testing	• maintenance and testing **must** be conducted at least every six months, and written records should be maintained	No comment	No change.
	Security Awareness Program	• all workers **must** receive security awareness training on a regular basis	No comment	No change.
	3.2 Technical Security Measures **3.2.1** **Requirements for technical security measures** Technical security measures for radioactive sources, devices or facilities **shall** include physical measures to: • prevent unauthorized personnel from gaining access to such sources • protect against an act or attempted act of unauthorized removal • protect against an act or attempted act of sabotage Technical security measures **shall** also include hardware and/or security systems designed according to the principle of defence in depth and the physical protection system functions of "detection, delay and response". This section includes security requirements for the following measures: • access control • detection of unauthorized access • locking hardware and key control • physical barriers (secure containers, secure enclosures) • alarm response protocols • inspection, maintenance and testing of physical security-related equipment • security officers Within each of the areas identified above, the licensee **shall** define appropriate security measures that are commensurate with the level of risk presented by the sealed source(s). Further details are provided in sections 3.2.2 to 3.2.8. In support of paragraphs 3(1)(g) and 3(1)(h) of the General Nuclear Safety and Control Regulations, the licensee **shall** include in their licence application details pertaining to physical security measures for access control, physical barriers, detection of unauthorized access, maintenance and testing of physical security-related equipment.		No comment	No change.

	3.2.2.1 **Requirements for access control** The licensee **shall** implement access control measures (e.g., access card readers, personnel identification systems, manual or electronic locks) or use security officers to ensure that only authorized persons have access to storage areas containing sealed sources at all times. Visitors, building maintenance staff, servicing companies 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.	No comment	No change.

7	**3.2.2.2** **Guidance for access control** To control access to the sealed sources, the licensee **should**: • prevent unauthorized access to the sources • 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 and biometric devices/systems, and through the use of "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 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, security officers).	Text Change.	Bullet 8 OPG seeks clarity to determine if duress signalling available to all Nuclear Security Officers (NSOs) while in hardened posts at the protected area boundary or while on patrol (by radio) would meet the requirement of signalling. While this duress signalling is not near the storage area, it is effective in directly alerting the Security Monitoring Room and NSOs. Bullet 9 OPG seeks clarity to determine if local alarming may be interpreted in a high security site as at the protected area. The protected area perimeter is equipped with alarming (dual detection) fences preventing unauthorized access and with alarming PM7 monitors that prevent unauthorized egress (using door interlocks) of any persons in possession of source material. While alarming is not in the vacinity of the storage area, it is effective in immediately alerting NSOs.for action.

8	**3.2.3.1** **Requirements for detection of unauthorized access** The licensee **shall** implement measures for the detection of attempted or actual unauthorized access in a timely manner, such as: • visual observation • video alarm assessment • detection devices • accountancy records, seals, or other tamper-indicating devices including process monitoring systems (for example, daily or twice-weekly audits, to ensure that the sources are present) 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; the monitoring station **shall** be certified by a body accredited by the Standards Council of Canada, or other certification body deemed acceptable by the CNSC staff • include an uninterruptible power supply subject to routine testing, to ensure continuous operability of the security detection system	No comment	No change.

	3.2.3.2 **Guidance for detection of unauthorized access** To detect unauthorized access, the alarm system **should**: • activate immediately upon detecting an intrusion or tamper event • stay in an alarmed state until acknowledged by an authorized person • have two or more zones for each area of storage • have an acceptably low nuisance and/or false alarm rate • be certified by the Underwriters Laboratories (UL) or Underwriters Laboratories of Canada (ULC) The licensee **should**: • ensure that alarm monitoring devices and back-up battery power are protected against tampering by unauthorized personnel (e.g., electronic panel or junction box) • ensure the keypad is installed within a secure environment, to prevent tampering • use dedicated alarm zones in the storage area (separate from any other alarm zones) and limit access to authorized users only • maintain an audit trail to record the cause of any alarms For example, consider a radiography company that has a warehouse equipped with an alarm system. Two zones are set up: one zone for the warehouse and a second interior zone for the storage area. During the day, the main alarm system for the warehouse is deactivated but the security system for the storage area remains activated and operates independently of the main system.	No comment	No change.

	3.2.4.1 **Requirements for 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 repairing or replacing a locking device, key, access card or combination that is defective, lost, stolen, or unlawfully transferred, or has otherwise become compromised.	No comment	No change.

	3.2.4.2 **Guidance for locking hardware and key control** The licensee **should** develop, maintain and adhere to written procedures for issuing, repairing or replacing a securing device, key, access card or combination that is defective, lost, stolen or otherwise compromised. 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 good quality. Key management procedures **should** be designed to prevent unauthorized access or compromise. The locks **should** have shielded shackles, to prevent cutting of the lock.	No comment	No change.

	3.2.5.1 **Requirements for physical barriers** For sealed sources whose activity is less than the threshold levels listed for Category 3 in Table A, the licensee **shall** store the sources in secure containers, as described in section 3.2.5.1.1. For sealed sources whose activity is equal to or above the threshold levels listed for Categories 1, 2, or 3 in Table A, the licensee **shall** implement a minimum of two different physical barriers, to prevent unauthorized access to sealed sources in storage or 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).	No comment	No change.

	3.2.5.1.1 **Requirements for secure containers** Secure containers include items such as filing cabinets, metal boxes, safes, 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]	No comment	No change.
	3.2.5.1.2 **Requirements for 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 nuclear substances and radiation devices 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.	No comment	No change.

	3.2.5.2 **Guidance for physical barriers** Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls and vaults are commonly used for storage of radioactive sealed sources. Barriers **should** be considered in relation to an adversary's objectives. The licensee **should** implement multiple physical barriers to protect the radioactive sources. Multiple barriers potentially force an adversary to bring a variety of tools to defeat each individual barrier, thereby delaying the adversary and providing the response personnel with time to intervene. One implementation of the concept of defence in depth is to have multiple layers of different barrier types along the path to complicate an adversary's progress by requiring a variety of tools and skills. 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 good quality padlock that has the same level of robustness (e.g., shielded shackles) • a solid-core door made of wood or metal, installed with non-removable screws, pinned door hinges, a latch protector and an automatic door closer • a window equipped with laminated window-film resistant to burglar attacks, metal mesh or metal bars spaced at 15 centimetres or less, and installed with non-removable screws	No comment	No change.

9	**3.2.5.2.1** **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., sledgehammer, crowbar, drill, blowtorch)	Text Change.	Given the significant security systems utilized at protected area perimeters of High Security sites, recommend rewording to indicate storage location and/or container **and/or facility perimeter** should be equipped with an alarm system to detect unauthorized entry or access.

	3.2.5.2.2 **Guidance for secure enclosures** Openings, such as windows or vent ducts, that could provide access to secure enclosures **should** be fitted with bars, a metal grill, expanded metal mesh, and/or retrofitted with a UL/ULC certified security film or glazing. Security hardware attached to windows **should** be affixed from the inside, to prevent tampering, or be fitted with tamper-resistant anchors if affixed from the outside. Doors that provide access to areas where radioactive sealed sources and/or radiation devices are used, processed or stored **should** be secured when unattended. The material used for the door **should** be solid-core wood or metal-clad, and the door **should** be installed in a reinforced frame of equivalent material. Doors **should** be in a good state of repair. If the hinges are mounted on the non-secure side, the door **should** be fitted with non-removable pinned hinges. Any door glazing or large vents (grills) **should** be fitted with security glazing or bars, a metal grill, or equivalent. Grills **should** be secured in place with tamper-resistant anchors. If continuous visual surveillance is done by an operator, the operator **should** be equipped with a means of communication (e.g., cell phone or radio) and **should** be aware of the response protocols to communicate rapidly to response personnel in the event of unauthorized access or removal. If key pads are used to arm and disarm an intrusion detection system, the device and its electric junction box **should** be installed in a secure area, to reduce the risk of tampering. To maintain continuous power to the alarm monitoring detection system in the event of a loss of primary power, the licensee **should** consider implementing an alternate or auxiliary power back-up source, or equivalent, to maintain detection capability.	No comment	No change.

	3.2.6.1 **Requirements for 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 police force of jurisdiction, 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.	No comment	No change.
10	**3.2.6.2** **Guidance for alarm response protocol** 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.	Comment.	Use of MOU for support arrangements in the local community by Police of Jurisdiction that have a duty to respond seems excessive. Recommend removal of MOU requirement.

	3.2.7.1 **Requirements for 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.	No comment	No change.
	3.2.7.2 **Guidance for inspection, maintenance and testing of security-related equipment** 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.	No comment	No change.

	3.2.8.1 **Requirements for security officers** If the licensee uses a security guard service, the licensee **shall** develop and maintain written procedures and instructions specific to: • measures for controlling access to the licensed area • surveillance foot and vehicle patrols • assessment and response to alarms • apprehension and detainment of unarmed intruders • report suspicious activities, including armed intruders, to the police force of jurisdiction • security equipment operation • security training relating to assigned duties	No comment	No change.
	3.2.8.2 **Guidance for security officers** 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 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.	No comment	No change.

	3.3.1 **General requirements for administrative security measures** Administrative security measures support technical measures, and **shall** include the programs, plans, policies, procedures, instructions and practices that the licensee implements to assist in securing licensed radioactive material from unauthorized removal or sabotage. These measures **shall** include, but are not limited to, the following: • site security plan • security awareness program • personnel trustworthiness and reliability • protection of prescribed or sensitive information • inventory control • access control procedures	No comment	No change.
11	**3.3.2.1** **Requirements for a 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 in accordance with section 12(1)(j) and 21 to 23 of the General Nuclear Safety and Control Regulations. The site security plan **shall** be updated and verified by the licensee at least once a year, to address any changes within the licensed facility.	Text Change.	Recommend annual FPS **review**, but actual update submission to CNSC is only when important changes are completed at the facility.
	3.3.3.1 **Requirements for a 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 training and awareness sessions **must** be maintained for all workers (as required by section 36(1) (d) of the Nuclear Substances and Radiation Devices Regulations). The security awareness program **shall** be documented and updated 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.	No comment	No change.

	3.3.3.2
	
	Guidance for a security awareness program
	
	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 [7].
		No comment	No change.

	3.3.4.1 **Requirements for 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 [8] 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 [8] **shall** be based on the category of the radioactive material. For Category 1, 2 and 3 sources, the licensee **shall**, at a minimum, verify the following information: a. confirm the identity of personnel from reliable original documentation such as passport or combination of other original documents (e.g., valid drivers license, health card or birth certificate) b. a record emanating from the Canadian Police Information Center, or from a police service servicing the area where the facility is located, showing the result of a criminal records name check (CRNC) on the person c. the person's employment history, including their educational achievement, and professional qualifications, unless the person has been employed for more than 10 years at the facility d. if a person's history cannot be established for at least the last five years, information relating to the trustworthiness of the person including, where available, a CRNC from each country in which the person has resided for one or more years in the last five years The licensee **shall** retain documentation regarding trustworthiness and reliability for a minimum of two years for current employees and **shall** protect the information in accordance with section 3.3.5.	No comment	No change.

	3.3.4.2 **Guidance for personal trustworthiness and reliability** These personnel screening practices are based on the personnel security standard in the *Policy on Government Security*, Treasury Board of Canada Secretariat [8]. The licensee's trustworthiness verification program **should** ensure individuals who have unescorted access to high-risk radioactive sealed sources are trustworthy and reliable, and do not pose an unreasonable risk to the health and safety of persons and security. The licensee **should** maintain copies of all documents provided by applicants and ensure they have been verified as original. The trustworthiness verification program **should** be reviewed on a regular basis. The trustworthiness verification program **should** apply to: • individuals with unescorted access to Category 1, 2 and 3 sources • vehicle drivers and those accompanying the transport of Category 1 sources • any individual whose assigned duties provide access to prescribed and/or sensitive information or the handling of Category 1 sources (including onsite security officers)	No comment	No change.
	3.3.5.1 **Requirements for 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.	No comment	No change.

	3.3.5.2 **Guidance for protection of prescribed and/or sensitive information** "Prescribed information" is defined in the *General Nuclear Safety and Control Regulations*, section 21 (see glossary). The following information is considered to be prescribed and **should** be protected: • 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 (i.e., "**PRESCRIBED INFORMATION**" or "**SECURITY PROTECTED**") in bold, upper-case letters • 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.	No comment	No change.

	3.3.6.1 **Requirements for 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 section 36(1) (a) of the *Nuclear Substances and Radiation Devices Regulations*.	No comment	No change.
	3.3.6.2 **Guidance for inventory control** The operator **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, or remote observation through closed circuit television (CCTV), or verification of seals or other tamper devices. A process for inventory control **should** be in place, to ensure a robust verification process.	No comment	No change.

	4 Security Measures for Sealed Sources during Transport **4.1 Vehicle Security** **4.1.1** **Requirements for 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., police agency of jurisdiction) 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.	**n/a - OPG contracts with qualified vendors to conduct all transport of sealed sources stated in Table A.** No Comment.	No Change.

	4.1.2 **Guidance for vehicle security** 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).		

4.2.1

Requirements for security measures for sealed sources during transport

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

As required by the *Packaging and Transport of Nuclear Substances Regulations*, the licensee **shall** provide the carrier with the appropriate shipping documents relating to the sealed source. The shipping documents shall include the corresponding description of security measures for sealed sources. Where more than one category of radionuclide applies (e.g., for shipments of multiple radionuclides) the applicable measures shall be based on the more restrictive category.

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

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

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

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

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

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

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

	4.2.1 Cont 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 • maintains 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.		

	4.2.2 **Guidance for security measures for sealed sources during transport** The licensee **should**: • provide security awareness training to all individuals engaged in the handling or transport of sealed sources, including refresher training when required • verify that, before transporting Category 1 and 2 sources, all persons employed by the carrier transporting the sealed sources 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 licensee's transport vehicles **should**: • be inspected by the licensee regularly for any signs of tampering or deterioration that **may** adversely affect their designated function • be tested by the licensee at least every six months • be inspected by a qualified operator 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 shielded and secured to the vehicle for safety and security.		

	4.3.1 **Requirements for the 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 specific Transport Security Plan to the CNSC at least 60 days before the anticipated date of shipment, for approval by the Commission Tribunal or a designated officer authorized by the Commission Tribunal • 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 police agency along the transportation route 9. the planned route 10. alternate routes to be used in case of an emergency		

	4.3.2 **Guidance for the transport security plan** 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		

	4.3.2 Cont e. proposed security measures • describe the measures used to monitor the movement of packages and/or conveyances containing radioactive sealed sources (e.g., global positioning system, vehicle tracking and monitoring system) • describe the measures used for escort, security searches, and procedures with response force in case of breakdown or a failure of the shipment to arrive at its destination at the expected time • describe the procedures to be followed during any schedule stop, or unscheduled delay during transport f. measures to monitor the location of the shipment g. provisions for information security • describe how the information will be protected • describe how this information will be communicated to individuals who need to know this information to perform their duties h. the communications arrangements made between the licensee, the carrier, and the consignee • describe the communication arrangements between the licensee, the consignor, the operator of the vehicle transporting the radioactive sealed source, and the response force along the transport route • describe how the licensee plans to ensure that communication coverage is adequate along the entire route • indicate the action to be taken if communication contact with a vehicle carrying a radioactive sealed source is lost i. communication arrangements made with any police agency along the transportation route • the licensee **should** ensure that all responsible police agencies along the transportation route are notified prior to transporting the shipment • the consignor **should** notify the consignee, in advance, of the shipment's departure time, the mode of transport, the expected delivery time and the allowable delivery period around that delivery time • the consignee **should** notify the consignor of receipt or non-receipt of the shipment within the expected delivery period j. the planned route • if the proposed route is to pass through an urban area, the licensee or applicant **should** describe the precise route to be taken through the area and how the shipment is to be schedule to avoid peak traffic times • include alternate routes to be used in case of an emergency		

	Appendix A: Sample Site Security Plan This appendix provides a list of topics to be considered when developing a site security plan.	No comment	No change.
	Glossary	No comment	No change.
	References	No comment	No change.
	Additional Information The following documents contain additional information that may be of interest to persons invloved in security measures for sealed sources.	No comment	No change.