Special Edition 2016

DNSR Newsletter

Canada's Nuclear Regulator

Security of sealed sources: What works, what doesn't and what's promising

The CNSC recognizes that both safety and security are intertwined and important in protecting sealed sources against malicious acts at every stage of their lifecycle. This special edition of the Directorate of Nuclear Substance Regulation (DNSR) newsletter provides relevant information on the security of sealed sources during storage and transportation. It focuses on promoting good security practices and outlines the security requirements of REGDOC 2.12.3, *Security of Nuclear Substances: Sealed Sources* while maintaining best safety practices. The CNSC believes that the implementation of proper safety and security practices in the management of sealed radioactive sources will minimize the potential for loss of regulatory control over those sources.

Why is it important to protect sealed sources?

From a security perspective, sealed sources need to be protected because they can be used to create radioactive dispersal devices (RDDs) if they are stolen. The contamination resulting from an RDD detonation would require a significant cleanup effort, including the possibility of demolition and reconstruction of buildings. It would also have a significant impact on the economic activities within and near the affected area. In addition, an RDD detonation could cause panic, fear, distrust and a loss of public confidence in the government as a regulator and the industry as an operator.

The CNSC has implemented regulatory requirements and licence conditions to protect the health and safety of workers, the public and the environment. CNSC licensees are required to follow these requirements – and it is their responsibility to implement measures to prevent unreasonable risk to people or the environment. Following the regulatory requirements and complying with all security measures will minimize the potential for the loss or theft of sealed sources.

Promising technologies

For both safety and security, some vendors are currently looking at integrating radio-frequency identification (RFID), global positioning system (GPS) and wireless technologies to improve the monitoring of exposure devices. Others are using satellite tracking system and geo-fencing to detect unauthorized removal and ensure safe overnight storage while they are out in the field.

Continued on page 2...

In this issue

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Security of sealed sources ...continued from p.1

Overview of past incidents and criminal threats

In many cases that involve the loss or theft of sealed sources, thieves have targeted unattended vehicles, often unaware that the vehicle contained nuclear substances.

From January 1, 2008 to October 31, 2015, there have been six events reported involving the loss or theft of high-risk radioactive sealed sources (i.e., Category 2) while in transport in Canada. In all cases the sealed sources were recovered shortly after the event occurred. In one case, the vehicle was stolen with the source stored inside; in another, a package carrying the source was reported as lost during transport when it was not delivered to the recipient on the expected date. One of the four remaining events was for a sealed source that was reported as missing from a medical device. For the final three cases, the sealed sources were not properly stored inside, not properly secured to the vehicle and lost during transport, and left at a previous job site.

Summary of security requirements under REGDOC-2.12.3

REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources*, includes the following requirements for licensees:

• Workers who have unescorted access to high-risk sealed sources (i.e., Category 1 and 2) must have undergone a trustworthiness and reliability verification, which includes a criminal record name check.
• All authorized users, including staff who transport high-risk sealed sources, must receive security awareness training on a regular basis.
• Vehicles must be equipped with anti-theft devices, including a vehicle-disabling device.
• Vehicles must be equipped with a minimum of two barriers to prevent unauthorized removal of the high-risk sealed source or device.
• Access should be restricted to authorized users only.
• Drivers must be equipped with proper means of communication in case of emergency.

Timelines for compliance

• May 31, 2015, for Category 1 and 2 sealed sources
• By no later than May 31, 2018, for Category 3, 4 and 5 sealed sources

International and industry best practices

The World Institute on Nuclear Security (WINS) has published an international best practice guide for the security of sealed sources used for industrial radiography (both in storage and in transport). This document – which was developed by industry practitioners and promotes a self-assessment methodology for identifying areas for improvement – is available on the WINS website.

In 2012, the Australian Nuclear Science and Technology Organization (ANSTO) held a regional workshop in Malaysia focused on improving the security measures for users of exposure devices. This workshop resulted in a report containing information and guidance (for both regulators and licensees) related to security practices for industrial radiography application, including a description of rcommended content of a security plan for users of exposure devices. This report, *2nd Sec Lev B Workshop, Malaysia, Dec 2012*, can be found on ANSTO's Regional Security of Radioactive Sources Project website.

Keep in mind

It's important to implement security measures to prevent loss or theft – but it's also important to plan for the worst-case scenario. Make sure your site security plan and procedures are ready and that your workers know what to do in case of a security incident. Regular security exercises and drills are a good way of testing equipment, procedures and worker response.

Continued on page 3...

Security of sealed sources ...continued from p.2

	What works	What doesn't
Training and security awareness	• Testing worker knowledge and providing them with a quick reference manual (e.g., security contact list, daily checklist for security verifications)	• Failing to provide workers with sufficient information about the security systems in place to enable them to perform their required duties and responsibilities with appropriate focus on security
Maintenance and testing of security systems	• Conducting routine maintenance verification and testing of security systems, including transport vehicles • Maintaining a log of routine maintenance verification for tracking repairs • Conducting performance testing	• Failing to identify and repair malfunctioning or unresponsive alarm system in a timely manner
Control of sealed source	• Maintaining constant surveillance (to the extent possible) of the sealed source while in storage and during every stage of transport; installing effective security systems can provide a reliable means of detection, especially if workers are aware of the system's capacity and limitations • Maintaining a two-person rule when transporting or using sealed sources is considered an industry good practice	• Failing to maintain constant surveillance or leaving the sealed source unattended while not being within range of the alarm; workers tend to lower their guard during lunchtime and breaks, which may provide opportunities for theft if the source or vehicle is left unattended
Tracking	• Tracking sealed sources at all stages of transport. GPS tracking systems on vehicles are required for Category 1 sources (as per section 4.1 of REGDOC-2.12.3) and a good practice for Category 2 sources	• Failing to keep track of sealed sources during shipments or after receiving new sealed sources
Key and lock control	• Maintaining effective control of the issuance of keys to transport vehicles and storage compartments	• Inadequate control and management of keys for vehicles and security padlocks
Physical security	• Implementing multiple physical barriers for deterring and delaying access to sealed sources (e.g., high-security padlocks that meet UL 437) • Implementing an alarm system with 24/7 response capabilities • Implementing compensatory measures when sealed sources are stored in vehicles overnight or at temporary job sites	• Using poor quality padlocks and security equipment that are easily bypassed with handheld tools • Installing contact switches on the wrong side of compartment doors
Response	• Implementing communication arrangements or response protocols with local law-enforcement agencies at the site, during transport and at temporary job sites • Providing familiarization visits to police and firefighter personnel on a regular basis • Performing security exercises with local law-enforcement agencies is an industry best practice for licensees with Category 1, 2 and 3 sealed sources	• Failing to communicate immediately with off-site local law-enforcement agencies • Having an inadequate or non-existant response protocol in case of a security incident

"The only thing necessary for the triumph of evil is for good men to do nothing." – Edmund Burke

Technical security measures for high-risk sealed sources and common security violations

To ensure that high- and medium-risk radioactive sealed sources (i.e., Category 1, 2 and 3) are secured properly during storage and transportation, licensees must implement several technical security measures. These measures must ensure that licensees can effectively detect a security breach and create delays in accessing the nuclear substance, and that they have implemented adequate response capabilities. Measures can include the following:

Effective access control measures to ensure only authorized users can gain access to sealed sources. (An authorized user is someone who has been cleared by the licensee as being trustworthy and reliable.) Part of an effective access control system is making sure non-authorized users are escorted at all times when onsite or in a secure zone.

Although many licensees have implemented electronic access control systems, CNSC inspectors have found that facility design and physical barriers are often overlooked. For instance, access control systems often do not take into account false ceilings, windows and ventilation openings. A person could use these as entryways to bypass the security system put in place to secure high-risk sealed sources – compromising the overall integrity of the security measures.

When transporting sealed sources, effective access control measures should prevent access to the sealed source as well as the vehicle. For example, access to vehicle keys and the sealed source storage compartment inside the vehicle should be restricted to authorized users only and kept under control at all times. Keys should not be left in the ignition and spare keys should not be hidden or stored inside the vehicle.

Measures for detection, assessment and response. In addition to deterring theft, these measures will also increase the likelihood of recovering sources if they are stolen. A variety of methods can be used, but the one chosen must include immediate detection capabilities. Means of detection, notification and immediate response must also be put in place for unattended vehicles with high-risk sealed sources inside.

For high- and medium-risk sealed sources, licensees should also have response protocols in place that include notifications sent to an approved call list from a monitoring station certified by the Underwriters Laboratories of Canada. For any actual or attempted theft, sabotage or diversion, licensees must have pre-established communication arrangements and/or response protocols with local law-enforcement agencies at the site, during transport and at temporary job sites. Having police and firefighter personnel visit licensed facilities on a regular basis will help them become familiar with sites and their hazards.

Two physical barriers to protect sealed sources at a facility or whenever they are in a vehicle. The objective is to delay access to the sealed sources by thieves and provide the licensee (and the police) with adequate time to respond to an intrusion.

At a licensed facility, two independent physical barriers might include:
• a locked storage container inside a locked storage room
• a locked storage vault or room within a locked and secured building

(Examples of physical barriers are presented on page 6)

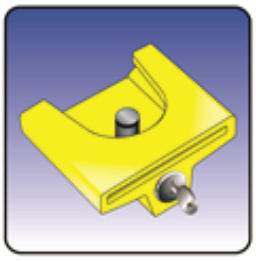
Continued on page 5...

Technical security measures for high-risk sealed sources and common security violations

...continued from p.4

When sealed sources are stored in a vehicle, two independent physical barriers could be a locked trunk, trailer or door serving as a second barrier to a locked storage container that is anchored and secured to the vehicle.

When high- and medium-risk sealed sources are in a vehicle, the licensee must also put in place a vehicle-disabling device. Many configurations are available, including trailer hitch locks (for sealed sources stored in a trailer), wheel locks (i.e., boots) or chains, and steering locks or the equivalent, all of which can delay and deter thieves. A kill switch or other similar device can be used to disable the vehicle's engine in the event that a theft has taken place.



Trailer hitch with lock

Wheel lock

Steering lock

Cover ignition kill switch

Common violations of security requirements

During compliance inspections, CNSC inspectors most commonly observe violations stemming from ineffective physical security measures and missing security documentation.

In some cases, licensees may have intrusion detection systems that function improperly, either because of poor preventive maintenance or inadequate verification and testing procedures. Licensees have a responsibility to test security alarms and ensure security systems are serviced and maintained on a regular basis (ideally, every six months). In other cases, intrusion detection systems are put in place but there is no immediate response in the case of an alarm. This usually occurs when there are no procedures or training for doing so, or when no one is within audible range of the alarm system when it is activated.

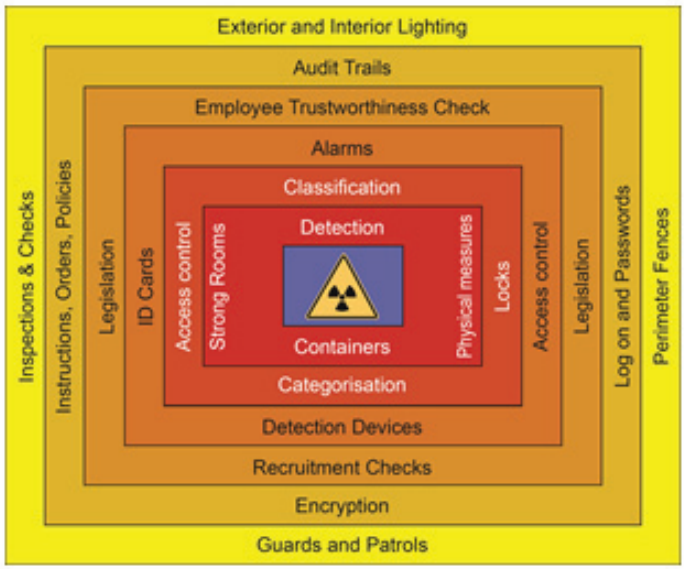
When implementing and maintaining their detection, notification and response measures, licensees must ensure all required elements are in place. Licensees, staff and operators should be well trained and aware of the security procedures and risks associated with working with sealed sources. They should also know about the potential dangers if security is breached and sealed sources end up in the possession of someone with ill intent. When implemented effectively, security measures should:

• deter potential thieves through security signage, surveillance cameras, barriers or human presence
• provide response personnel with sufficient time to act following detection
• ensure detection is combined with an assessment strategy to verify the cause of the alarm and notify response personnel in case of a security event

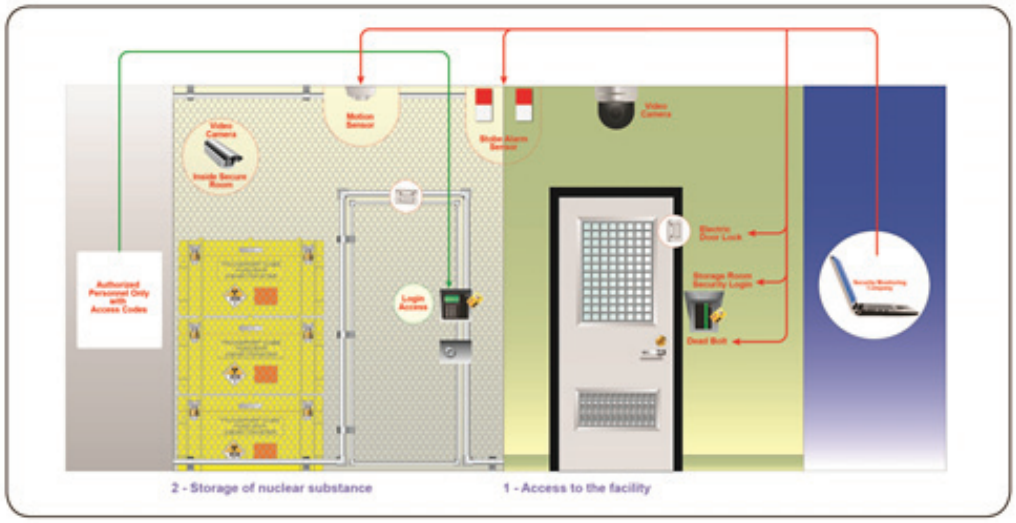
Continued on page 6...

Technical security measures for high-risk sealed sources and common security violations ...continued from p.5

• ensure the time delay provided by the physical barriers is greater than the time required for notification and response
• employ balanced protection to ensure the security functions (e.g., deterrence, detection delay, response, security management) provide adequate protection against all threats
• implement a defence-in-depth approach as illustrated below:



Finally, the most common security violation is usually found when assessing a licensee's site security plan. In such cases, CNSC inspectors often find that plans do not accurately describe the security procedures used by the licensee, for both new site security plans (for proposed licensed locations) and existing site security plans. In some cases, the transportation and site security programs have changed or are not following the site security plan; in others, there is a lack of security awareness training or alarm-testing records.



Example of two physical barriers at a facility

Licensees possessing Category 1, 2 or 3 sources: Requirements for employee trustworthiness checks

The following is adapted from section 3.3.3 of REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources*.

The requirement

Licensees in possession of high-risk radioactive (Category 1, 2 or 3) sources must implement an effective program to verify that personnel with unescorted access to these sources are trustworthy and reliable. The trustworthiness check's main objective is to ensure that individuals with unescorted access to sources do not pose an unreasonable risk to public health and safety. The check includes:

• employment and education background checks
• confirmation of the person's identity, using reliable documentation
• a criminal records name check

Personnel who require access to high-risk radioactive sources in order to perform their jobs, but who are not approved by the licensee (e.g., students, contractors, building maintenance, concierge), must be escorted by an approved individual.

The risk

The trustworthiness check is intended to reduce the risk of an insider threat – for example, an employee with authorized access who might attempt to steal, tamper with or sabotage radioactive sources.

The decision to grant, deny or revoke unescorted access rests with the licensee. This decision should be supported by a management policy that includes a decision-making process based on risk.

The licensee should implement controls to protect individuals' information from unauthorized disclosure. This information should be stored in accordance with federal and provincial regulations.

The responsibility

Licensees are responsible for evaluating the information required to determine if an employee is trustworthy and reliable enough to be given unescorted access to high-risk radioactive sources. As part of this process, licensees should identify their own specific criteria for determining trustworthiness and reliability by verifying references, education, work experience, criminal background checks and government-issued identification. Criteria to assess criminal background checks could be based on the type, frequency, age, date and seriousness of any criminal convictions. 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 resulting in conviction
• indication of deceitful or delinquent behaviour
• attempted or threatened destruction of life or property
• illegal drug use, abuse or distribution
• history of alcohol abuse
• failure to comply with work directives
• hostility or aggression toward fellow workers, authority figures or anyone else
• violation of safety or security procedures

Continued on page 8...

Licensees possessing Category 1, 2 or 3 sources ...continued from p.7

These indicators are not all-inclusive, but are examples that may be considered. They are also not intended to be disqualifying factors for employment. Licensees should consider extenuating or mitigating factors, as well as the accumulation of multiple indicators, when deciding whether to grant unescorted access to radioactive sources. Ultimately, it is left to the licensee to deem whether a person's history is unreliable or untrustworthy, and if he or she represents an unreasonable risk to the security of radioactive sources.

Security inspections performed by the CNSC Staff

The CNSC's Operations Inspection Division (OID) and Accelerators and Class II Facilities Division (ACFD) regularly inspect licensees in possession of Category 1, 2 or 3 sealed sources. Inspections are typically conducted to verify compliance with regulatory requirements for the safe use of nuclear substances, and they examine areas such as radiation protection, transportation, operational procedures, and training and qualification.

In May 2013, the CNSC approved REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources*, which informs licensees of their minimum security requirements for sealed sources. OID inspectors have been performing routine inspections since early 2013 to verify the security-related requirements outlined in REGDOC-2.12.3, and to make recommendations to licensees about this document until it is fully implemented in 2018. In the past, security advisors from the CNSC's Nuclear Security Division had performed these verifications. By making this change, the CNSC hopes to reduce the regulatory burden on licensees by combining safety and security inspections into a single inspection.

Licensees with Category 1, 2 or 3 sealed sources may still have a separate inspection conducted by a security advisor if they want to add a new location or make significant changes to a location where these sources are being stored, or if the aggregate quantities of Category 4 and 5 sources are at or above the activity levels for Category 3 sources. Security-related inspections verify compliance with applicable regulatory requirements and confirm that licensees are adhering to their commitments to the CNSC as outlined in their security plans.

As part of the inspection process, licensees are required to have a copy of their current and approved site-specific security plan available for the inspector to review while onsite. The inspector will also verify access controls, information security, security awareness training, and confirm the secure storage of sources.

Findings related to the safety of nuclear substances are left onsite or otherwise communicated to the licensee shortly after the inspection. Any security-related findings are presented to the licensee in a separate report at the time of the inspection. This report and all subsequent communication about these findings are classified as "Confidential – Prescribed Information" and must be treated as such by the licensee. This means that the information must be secured and shared with others on a need-to-know basis only. In addition, correspondence must be sent to the CNSC in hard copy via mail or courier only, as normal fax and email are not acceptable for communicating information classified at this level.

Through the careful management of security-related information and by implementing the necessary security measures to protect nuclear substances, licensees are doing their part to prevent the theft, sabotage or loss of high-risk nuclear substances.

Case study: Theft of sealed sources

On June 20, 2013, a truck transporting a portable gauge was reported stolen in British Columbia. The police were immediately notified of the incident, along with the CNSC duty officer and licensing specialist. Although the truck was found down the street shortly thereafter, the contents of the truck – including the gauge – were not recovered. The gauge was supposedly secured in a lockbox with a tonneau cover in the back of the truck.

Humboldt HS-5001EZ moisture-density gauge

Upon notification of the event, CNSC staff contacted both the Royal Canadian Mounted Police (RCMP) and the United States Nuclear Regulatory Commission. The International Atomic Energy Agency (IAEA) was also notified and the event was inserted into the Incident and Trafficking Database: the IAEA's information system for illicit trafficking and other unauthorized events involving nuclear material as well as other nuclear substances no longer under regulatory control.

A few days later, the RCMP published a press release to inform the public of the risks associated with coming into contact with the gauge and to request assistance in finding it.

On July 4, 2013, the gauge was found in a wooded area near the location where the truck was previously recovered. Fortunately, the gauge was intact and still in its locked transport container. However, the container had been easily removed from the truck because it was not chained to the vehicle, as required in the licensee's internal security procedure.

Following the event, the licensee provided refresher training to employees to remind them that the gauge must be secured in the proper storage area. The training also reinforced the need to follow the licensee's security protocol and policies – and the security consequences of not doing so.

Which security measures worked?

In this case study, it is clear that the following security measures were effective:

- having a response protocol in place that involved immediately notifying the police and CNSC
- informing the local community and media about the event and asking their help to find the vehicle
- sharing lessons learned with licensee staff at all their locations
- improving security awareness training, procedure, as well as security measures

These actions were ineffective toward maintaining security:

- not following internal procedures and processes to secure the gauge properly
- not having quality control verification and redundant verification (i.e., a two-person rule)
- failing to maintain constant control and surveillance of the vehicle containing the gauge

What we can learn from this case study

Similar instances of lost or stolen gauges are reported each year to the CNSC. Of the 110 gauges reported missing between January 1, 2008 and October 31, 2015, approximately one-third (36) were moisture-density gauges. Theft or loss typically occurs when these gauges are being transported or when they are being stored at a construction or temporary job site. In most cases, the vehicle is targeted by thieves who are unaware that a gauge containing radioactive nuclear substances is inside the vehicle.

Continued on page 10...

Case study: Theft of sealed sources ...continued from p.9

To prevent similar events from occurring, licensees must always implement prudent management practices for lower-risk (i.e., Category 4 and 5) sealed sources. For example, when a gauge is onboard a vehicle, security awareness training must be given to employees working with the gauge to promote safe and secure practices. Licensees should also put in place physical deterrents (e.g., locks, padlock, chains) and maintain constant surveillance and control of their gauges at all times. All security measures for high- and medium-risk sources must meet the minimum requirements stipulated by the *General Nuclear Safety and Control Regulations* and REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources.*

Vehicle GPS and tracking systems for transporting Category 1 and 2 high-risk radioactive sealed sources

High-risk sealed sources (i.e., Category 1 and 2) are generally at a higher risk of being stolen or lost when being transported by vehicle. To secure these sources during transport, it is important to:

- ensure drivers are trustworthy
- ensure drivers can communicate immediately with local law-enforcement agencies (e.g., cellular phone, two-way radio)
- perform regular inventory checks on sources stored in vehicles
- notify the recipient of shipment details, including arrival time and date
- confirm delivery and receipt of the shipment if using a third-party carrier
- notify the appropriate agencies in case of a security event such as loss, theft, malevolent acts or any incident involving nuclear substances
- use global positioning system (GPS) tracking for Category 1 sources and an appropriate tracking system for Category 2 sources
- develop and implement a transport security plan

It should be noted that a “specific” preliminary transport security plan is required for Category 1 sealed sources. This plan must include all available information – mode of transport, planned route, proposed security measures, measures to monitor shipment location and communication arrangements with off-site response – and be provided to the CNSC 60 days before the anticipated shipment date. A final transport security plan, including supplementary information unique to each shipment, must be submitted to CNSC 48 hours before the shipment occurs.

A “generic” transport security plan is required for Category 2 sources and can be part of the licensee’s site security plan.

What is an appropriate tracking system?

An appropriate tracking system is one that allows the licensee to monitor the movement of sealed sources. In addition to helping determine if a shipment has been lost, misplaced or stolen, a tracking system will provide information related

Continued on page 11...

Vehicle GPS and tracking systems for transporting Category 1 and 2 high-risk radioactive sealed sources ...continued from p.11

to a shipment's last known location as well as the time and date when it was last seen, which may assist in the recovery and follow-up investigation. A tracking system does not necessarily have to be an active monitoring system, like a GPS tracking device.

Technologies used in tracking systems

With a GPS system, vehicles are tracked in real time by radio frequency, which can be used during an active investigation to locate a stolen vehicle. Other technologies, such as two-way satellite monitoring systems, allow licensees to monitor shipments remotely through a secure website. This type of technology sends alerts directly to a computer or mobile device via email or text message. It can also provide tracking, intrusion detection or tamper-detection capabilities, along with remote site monitoring.

Another technology, geo-fencing, establishes a predetermined transportation path – and then alerts the licensee when deviations from that path occur. There are also radio-frequency identification (RFID) solutions, which contain electronically stored information and can use either passive or active devices to keep track of sources. Some RFID solutions are powered by battery, work with wireless networks and can integrate with GPS systems. This technology is developed for cellular GPS tracking on vehicles and can be used for inventory control, mapping and geo-fencing.

It is important that licensees implement adequate security measures to maintain control of high-risk radioactive sealed sources during transport. This will allow them to be immediately notified of any unplanned event, which may reduce the amount of time it takes to notify law enforcement or first responders in case of an emergency or security event.

International and industry best practices for tracking systems

The World Institute on Nuclear Security and the World Nuclear Transport Institute have published an international best practice guide for government agencies, regulators, licensees, carriers and law-enforcement officers titled *Electronic Tracking for the Transport of Nuclear and Other Radioactive Materials*. This guide also provides a high-level description of the potential merits, challenges, viability and effectiveness of electronic tracking systems, which should help stakeholders select the most appropriate tracking method for their shipments.

GPS monitoring.

DNSR Newsletter

The *DNSR Newsletter* is a CNSC publication. If you have any suggestions on topics or issues that you would like to see covered, please do not hesitate to contact us.

ISSN 1920-7484 (Print)
ISSN 1920-7492 (Online)

Canadian Nuclear Safety Commission
P.O. Box 1046, Station B
Ottawa, Ontario K1P 5S9
Telephone: 1-800-668-5284 (in Canada)
or 613-995-5894 (outside Canada)
Fax: 613-995-5086
Email: cnsc.information.ccsn@canada.ca
Web site: nuclearsafety.gc.ca