Performance-Based Approach to the Security of Radioactive Sealed Sources*:* A Canadian Perspective

Raphaël Duguay, M.Sc., PSP
Nuclear Security Division
Canadian Nuclear Safety Commission, Canada
raphael.duguay@cnsc-ccsn.gc.ca

Abstract

In 2013, the Canadian Nuclear Safety Commission (CNSC) published a regulatory document *REGDOC 2.12.3* to enhance the security of radioactive sealed sources in Canada. This regulatory document is based on the security recommendations of the International Atomic Energy Agency's *Code of Conduct on the Safety and Security of Radioactive Sources* and related documents in the *Nuclear Security* series, and follows a risk-based approach using a performance-based regulatory framework. This paper provides the reader with a Canadian perspective o the security of radioactive sealed sources, and a reflection on those security measures and practices that have proven to work effectively, as well as those that look promising from a security management and physical protection standpoint.

Note on Terminology: In this paper, the term "performance-based" means focusing on setting a goal (or an objective) without proposing any specific means to achieve it. Also, the term "radioactive source security" is used in relation to a physical protection program that includes technical and administrative security measures and practices to prevent the theft, loss, or sabotage of radioactive sources that could be used for malicious purposes. It does not include import and export controls, or safety measures used for radiation protection, detection instruments, or emergency response.

Background

After the terrorist attacks of September 11, 2001, the CNSC adopted a strategy to enhance physical protection of nuclear facilities throughout Canada and in particular high-security sites. The CNSC Nuclear Security Division was expanded to include a group of security specialists mandated to conduct field inspections at those licensee facilities authorized to possess high-risk radioactive sealed sources. Due to the absence of specific security regulations for radioactive sealed sources, the CNSC used a performance-based approach, and worked closely with industry and licensees, to identify potential vulnerabilities in their physical protection systems and explore solutions to reduce risks. (One example: device hardening to increase the adversary's efforts, increasing the adversary's risk of being apprehended by enhancing security detection and assessment systems, and/or extending patrols and surveillance).

Performance-based regulatory approach

In 2006, the CNSC began developing a regulatory document[1] for the security of radioactive sealed sources, based on the International Atomic Energy Agency's (IAEA) *Code of Conduct on the Safety and Security of Radioactive Sources.* The purpose of this regulatory document is to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of radioactive sealed sources while stored at an authorized location or during transport. The adopted regulatory approach includes both prescriptive and performance-based language. In addition, this document identifies a clear objective and the criteria to achieve compliance, and provides guidance to licensees to assist them in finding appropriate security solutions, commensurate with the category of their radioactive sealed source (based on the IAEA *Categorization of Radioactive Sources* and the associated security level). For example, a performance-based requirement states that "the licensee must implement a means to detect unauthorized access", but does not specify the means (which can rely on either human activity or electronic measures).

It is my opinion that the performance-based approach permits implementation of security measures providing the licensee and the regulator with flexibility in the manner in which they seek to meet international standards for source security/protection. In the initial phase, the approach consisted of setting applicable security objectives and focusin on the end-result—or the effectiveness—of the process. Many Canadian licensees did not possess the necessary technical security expertise and there was limited guidance, so security specialists from the CNSC were utilized to help identify effective and acceptable solutions. After the initial inspections and the implementation of additional security measures, the licensees gained sufficient experience to implement solutions (specific to their operations and locations) to meet the regulatory requirements. In the initial phase, the focus was primarily on high-risk radioactive sealed sources. This approach was developed to allow flexibility for the licensees and the industry as a whole, recognizing that "one size does not fit all" when implementing security measures. The strategy allows the licensees to: gain knowledge and experience by developing their security program; and take different initiatives to achieve compliance without compromising safety or security.

Canadian approach: A mix of performance-based and prescriptive regulatory requirements

The Canadian model for the regulatory documentation concerning the security of radioactive sources is based on the security recommendations of the IAEA *Code of Conduct on the Safety and Security of Radioactive Sources* and IAEA Nuclear Security Series. During the development of this document, CNSC staff consulted other government agencies responsible for regulating dangerous goods (such as explosives, biohazards and chemicals agents). CNSC also consulted other countries, to ensure the alignment of security requirements and avoid regulatory conflicts (which may impede the trade and transportation of radioactive sealed sources across borders).

[1] REGDOC 2.12.3, *Security of Nuclear Substances: Sealed Sources* (2013).

As a result, a performance-based approach was implemented for security measures during the entire lifecycle from their manufacture until their safe disposal including while they are in storage and/or transport. In some areas, the CNSC used more prescriptive language to identify minimum requirements to prevent inadequate measures (e.g., retention of training records, testing frequency of alarm systems, site security plans, arrangements with offsite responders, and conducting trustworthiness and reliability verifications).

Operational experience: What works?

Performance-based inspections and associated compliance activities

It is my opinion that security inspections focused on performance, allowing both the regulator and the licensee to assess the effectiveness of a physical protection system and its vulnerabilities, have considerable merit. For example, during an inspection, the inspector may ask the licensee to test the intrusion detection system at the site where the radioactive sealed source is stored, in order to collect information on the time taken for detection, assessment, delay and response. At this stage, the devices or process vulnerabilities will be reviewed and tested to see if they compromise the overall objective of the security system.

Facility security plans are another example where feedback and comments from the regulator proved beneficial to the licensee. Although it may appear to be prescriptive in nature (because it is usually included as part of a license condition or a regulatory requirement), the responsibility in the development and implementation of this document belongs to the licensees. The consultation process is another instance where the regulator may help the licensee identify areas of improvement, and avoid non-compliance during inspections. This is particularly beneficial for licensees who submit security system designs and plans for specialists from the regulator on whether the proposed design meets the security requirements. During the site security plans reviews, it is possible to identify gaps related to mandatory requirements and missing information that support the security program. For example, missing information on the frequency of security devices maintenance and security awareness training should be documented to provide records that they are being implemented and maintained in accordance with requirements.

Working with the industry associations and licensees

It is my experience that some licensees lack security experts or have limited knowledge of physical security systems. Security specialists from the regulatory body are available to provide additional assistance and support in identifying vulnerabilities, as well as options to mitigate risks and meet requirements.

Security specialists are also involved at the construction phase of a new license facility (i.e., new build) or when a licensee is relocating or opening a temporary job site to a new location. In these instances, security advisors assist the licensees (or contractor) to identify the appropriate security measures that must be implemented before the site is ready to possess the radioactive sealed source. This approach often results in licensees saving on

expenses related to physical security enhancements that were not included in the initial budget.

During the development of this regulatory document, industry was consulted extensively, and encouraged to take proactive steps to address the updated security objectives. CNSC security advisors also met with licensees, to assist them in finding solutions that met the regulatory expectations. This experience has proven to be very effective in establishing strong communications and good relations with the licensees.

New licensees can also contact CNSC's security advisors to get an understanding of the requirements and to obtain clarification on the *Nuclear Security Regulations* and the CNSC expectations. In some cases, the CNSC provided assistance to the licensees in establishing contact with the appropriate local law enforcement authorities to facilitate the exchange of information and development of response arrangements to security incidents.

Case Studies: Communicating with the industry

Oil well logging and radiography companies occasionally work in remote locations, with a reduced presence of law-enforcement agencies and security contractors. In such situations, security systems can be expensive, and certain technologies may be unavailable. Following consultations with the regulator, some companies implemented equivalent security procedures (such as the "two-person rule", constant human surveillance, improved communication practices) to maintain control of the source during operations. The intent is to avoid unreasonable costs and implement a balanced solution, which still meets security requirements.

The consultation process was transparent and open for public comment. During the process, the industry asked for additional guidance on criminal record name checks (CRNC). The regulator provided more detail and suggested reliable CRNC alternatives. This flexibility allows the licensees to save on costs and avoid duplication on rules and requirements coming from different regulatory agencies. For example, a Canadian firearm acquisition license requires a thorough background verification, which is completed by a law-enforcement agency and can be used as a CRNC equivalent.

What's promising?

Threat and risk assessment, adversary pathway analysis and security self-assessment

In collaboration with the CNSC, some members of industry conducted security self-assessments, adversary pathway analyses, and/or threat and risk assessments specific to their site or activity. These assessments are recognized as good practices[2] as they helped the licensees identify potential threats and vulnerabilities specific to their sites. It is my

[2] The World Institute of Nuclear Security (WINS) has developed a series of Best Practices documents that also encourage the use of self-assessment methodologies to identify gaps and weakness in a security program.

opinion that this approach allows the licensees to implement reasonable security measures, commensurate with the level of risk associated with their licensed facility.

Unannounced performance testing of security systems, procedures and personnel

It is my experience that some licensees have taken a proactive stance, by implementing more thorough unannounced verification to ensure the readiness of systems, processes and personnel. This practice is a very effective tool in identifying vulnerabilities in physical security systems, access control, and other internal processes and procedures. In other cases, the licensees conducted performance testing of their security equipment and response personnel, to ensure timely detection, assessment and response, without having any operational impact on the site.

Involving management and other stakeholders in security

In some cases, licensees have created special security committees for the protection and management of radioactive materials at their site. These committees were also responsible for addressing security issues related to information technology, transport, trustworthiness and verification, training, workplace violence, personnel, etc.

One medical facility licensee created a multi-disciplinary team (including personnel designated for radiation safety, security, fire safety, a medical treatment team and a building manager) to ensure that all necessary considerations are taken into account when implementing security upgrades. It is my opinion that this integrated approach to security, which also involved management, was an adequate means to manage risks and to promote workplace safety and security culture.

Security awareness training and promoting security culture

To ensure effective and regular training, most public facilities have included security awareness in the mandatory annual safety and radiation protection training. To ensure compliance and good practices, security awareness is now integrated into a mandatory refresher training courses and safety manuals, and is provided to onsite security personnel. In some cases, members of the local law enforcement agencies were invited to a familiarization tour of the site and to get basic security and safety training.

Some licensees are quite innovative in using social media and communication tools. One licensee, for example, published a monthly security bulletin and was very proactive by doing fund raising for non-profit organizations in parallel with security awareness activities. To motivate its employees and increase worker participation, the licensee distributed security quizzes and rewarded the best participants with prizes. The employee participation in these events was strong, and provided an excellent opportunity to improve the security culture and raise funds for a good cause.

International efforts

Several international initiatives are being implemented by the IAEA to increase security awareness and training of individuals involved in the security of radioactive sealed sources. Canada has taken part in these efforts, for example, by providing early support and assistance both domestically and to international partners. These global initiatives provide

excellent opportunities for exchanging information on best practices, as well as for conducting professional networking.

Learning from best safety practices

The Canadian nuclear industry has training programs on safety and radiation protection as part of mandatory requirements. When new security requirements were implemented, they were also integrated into the licensee training program. Some licensees already followed stringent inventory control measures and security verifications that were easy to implement. For transportation security, the containers' safety design (such as shielding, weight, size) already included robust security features, which are difficult to defeat and provide additional level of security.

Challenges

- Identifying roles and responsibilities: because of the multiple licensees' representatives, it is at times difficult to define specific roles and responsibilities and to identify who is responsible fo the security of radioactive sealed sources.

- Potential for duplication: because of multiple requirements from various regulators, it is important to avoid duplication with other government agencies, resulting in unnecessary financial burdens and costs to the industry.

- Finance/Cost: Some licensees have difficulty finding the financial means to enhance physical security. It was important to address "operational needs" and to implement reasonable measures to assist the operator in meeting requirements without imposing a financial burden and without impeding their core operations (i.e. hospital environment). However, the licensee must implement compensatory measures if they are not meeting the requirements.

- Public and semi-private facilities: Facilities that are open to the public pose particular security challenges. For instance, universities and hospitals have more difficulties in implementing surveillance, access control measures and in identifying and assigning responsibility for security and response. As such, it is important to work with the licensee, to establish good security practices and promote an effective security culture. These facilities are considered to be "soft targets", and controlling access and conducting trustworthiness and reliability verifications for students, foreign researchers or third-party service providers may be a challenge. In addition, medical facilities need to balance security with patient safety, patient privacy and movement of sources within the facility.

- Remote locations: Response times of law-enforcement agencies are longer when high-risk sealed sources are transported and/or stored in remote locations. The effectiveness of security technologies for detection and assessment may also be challenged by the location's geographical features and/or inclement weather conditions.

- Safety/Security: One of the biggest challenges was to ensure that security controls did not adversely affect safety measures and practices and vice-versa. Throug experience and case studies, the CNSC identified several potential conflicts between safety and security, and worked toward finding balanced solutions, to ensure both of these were properly addressed.

- Sustainability/Security Culture: Continuous security awareness and promoting a sustainable security culture continues to be a challenge, particularly when it comes to protecting radioactive sealed sources against malicious use. Some licensees see security as an unwarranted expense against non existent threats, or assume that their remote location provides sufficient protection. Promoting continuous security awareness and a proper sustainable security culture continues to be a challenge.

It is the my opinion that despite the challenges of implementing security enhancements and developing a robust security program, working in collaboration within industry allows everyone to achieve the same goal and enhance the security of all radioactive sealed sources.

Lessons learned and recommendations

It is my opinion that:

- It is important to work closely with the industry and licensees to design and implement effective security measures. It is also important to address their concerns and questions, and share best practices in the field. For example, CNSC-sponsored workshops on industrial radiography are held annually, to discuss licensing and compliance expectations and current issues related to this field of activity. The regulator also publishes information bulletins, to promote awareness and exchange of information. It was also noted during field inspections and desktop reviews that the compliance rates were higher when the licensees were engaged in an outreach activity or another form of communication with the CNSC.

- Regulatory compliance verifications and performance-based inspections related to radioactive source security are now routinely conducted by safety inspectors. Safet inspectors receive basic training on security measures and regulatory requirements. In general, the first initial security assessment is conducted by a security expert for ever new location or new operating licence. Safety inspectors conduct follow-up field inspections and unannounced verifications to ensure that the licensee has an effective safety and security program which meets all the regulatory requirements. This approach may prove to be more sustainable in the long-term, but requires cooperation, planning, structure, and routine security-awareness training for safety inspectors.

- Although Category 1, 2 and 3 radioactive sealed sources[3] are considered to be the most dangerous, it is important to ensure good security and prudent management practices for low or very low-risk radioactive sources (category 4 and 5). This is the approach taken during the security awareness training provided to inspectors from the CNSC, as well as in the regulatory documents that provide requirements and/or guidance to licensees.

- Guidance documents should be more specific for different source use types, and provide more details to licensees. For example, a licensee in the medical sector should have access to guidance documents and technical references that can help them implement, design and maintain a security program to protect their radioactive sealed sources. These can have multiple applications and some may pose unique challenges including; radiation protection, patient safety, or mobile sources.

[3] International Atomic Energy Agency (IAEA) Categorization of radioactive sources, IAEA TECDOC-1344, July 2003.