Security Measures for Radioactive Sources

Challenges for Chalk River Nuclear Laboratories

2018 January 24

Our Brief History

www.cnl.ca

- Chalk River Nuclear Laboratories (CRNL) was created in 1944
- In 1952, Atomic Energy of Canada Limited (AECL) was created by the government to promote peaceful use of nuclear energy. AECL also took over operation of Chalk River from the NRC.
- CRNL is a site of major research and development to support and advance nuclear technology

Our Brief History

www.cnl.ca

- In 2015 AECL transferred management and operations to the Canadian National Energy Alliance and CRNL became Canadian Nuclear Laboratories (CNL).
- CNL is Canada's premier nuclear science and technology organization. CNL is a world leader in developing peaceful and innovative applications from nuclear technology.
- Over the next decade, CNL will be transforming its Chalk River Laboratories (CRL) through the revitalization of essential site infrastructure, the decommissioning of aging infrastructure and a significant investment in new, world-class science facilities

Canadian Nuclear Safety Commission

Mandate of the CNSC

The Canadian Nuclear Safety Commission regulates the use of nuclear energy and materials to protect health, safety, security and the environment; to implement Canada's international commitments on the peaceful use of nuclear energy; and to disseminate objective scientific, technical and regulatory information to the public.

Canadian Nuclear Safety Commission

Changes to the Regulatory Requirements for Sealed Sources

- Draft Regulatory Standard S-322 Physical Security Requirements for the Storage of Sealed Sources issued in November 2006.
- Draft Regulatory Standard S-338 Physical Security Requirements for Sealed Sources during Transport issued in November 2006.
- REGDOC – 2.12.3, Security of Nuclear Substances: Sealed Sources was released in 2013 May and replaces S-322 and S-338.

Canadian Nuclear Safety Commission

RegDoc 2.12.3 Content

- Sets out the minimum security requirements that must be implemented to:
- prevent loss,
- sabotage,
- illegal use,
- illegal possession,
- or illegal removal during their entire lifecycle, including while in storage, transport, or being stored during transportation.

Challenges

- Increased from 3 Categories to 5 Categories.
- Two years from date of issue to implement requirements for Category 1 and 2 (May 2015).
- Five years from date of issue to implement requirements for Category 3, 4 and 5 (May 2018).
- Aging infrastructure
- Identified as a high security site
- Aggregated quantities
- Department and Employee engagement
- Developing a security plan to meet the requirements
- Developing a transportation plan to meet the requirements

On Site Inventory

Over 500 sources on site that must be secured.

- **4 active Cat 1, 1 inactive Category 1**
- **9 active Cat 2**
- **9 active Cat 3, 4 inactive Category 3**
- **302 active Cat 4, 5, 211 inactive Cat 4, 5**

Active are in use

Inactive are disposed/decayed/shipped off

RegDoc 2.12.3

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
Access Control: • restrict access to authorized user only. • two-person rule (optimal) Cat 1 only • visitors, students, contractors must be escorted at all times by an authorized user.	• Sources are stored and used in shared lab areas. • As a research facility CNL supports many visiting researchers and students.
Intrusion detection system: • must provide immediate detection and be linked to a control room monitored by an operator 24/7 or an equivalent mechanism.	• Sources are located in multiple facilities. • Aging infrastructure doesn't support immediate detection.

RegDoc 2.12.3 continued

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
Perimeter and/or physical barrier: • must be protected with at least two physical barriers (i.e., walls, cages, secure containers) to separate the source from unauthorized personnel and provide sufficient delay to allow for immediate detection.	• Ensuring at least two physical barriers that met the requirements for sufficient delay. • Immediate detection.
Security of storage: • secured with high quality padlock, high security lock or equivalent security system. • secure containers must be able to resist an attack by handheld tools.	• Certain sources couldn't be secured with a locking device. • Ensure the Custodian requesting sources has the proper security requirements in place prior to receiving.

RegDoc 2.12.3 continued

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
Mobile Sources: • mobile sources in use, must have continuous visual surveillance by operator personnel.	• Ensure source Custodian understands the requirements and have proper arrangements in place.
Response Protocol.	• Minimal Challenge based on established response force on-site.
Personal trustworthiness or background checks.	• Minimal Challenge based on current site entry requirements.

RegDoc 2.12.3 continued

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
Information security: • all prescribed information must be protected and be shared on a need to know basis.	• Minimal Challenge based on current site policies for the protection of information.
Inventory Control: • 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.	• Not all sources are easily accounted for based on storage or usage. • Must introduce a system to ensure inventory controls are met.

RegDoc 2.12.3 continued

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
Security awareness program: • all authorized users, including staff who transport radioactive sources, must receive security awareness training on a regular basis.	• No formal program in place for Custodians, Logistics and Transport Carriers.

RegDoc 2.12.3 continued

Security program sub sections For Category 1 and 2 sources

Requirement	Challenge
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. • drivers must be equipped with a means of communication in case of emergency. • two-person rule (optimal)	• Ensure the Carrier meets and maintains the requirements of the regulations.

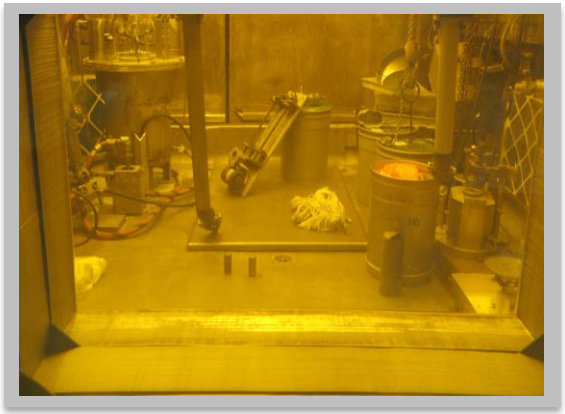
Source Usage

Gamma Cells

Challenge for inventory control and securing.

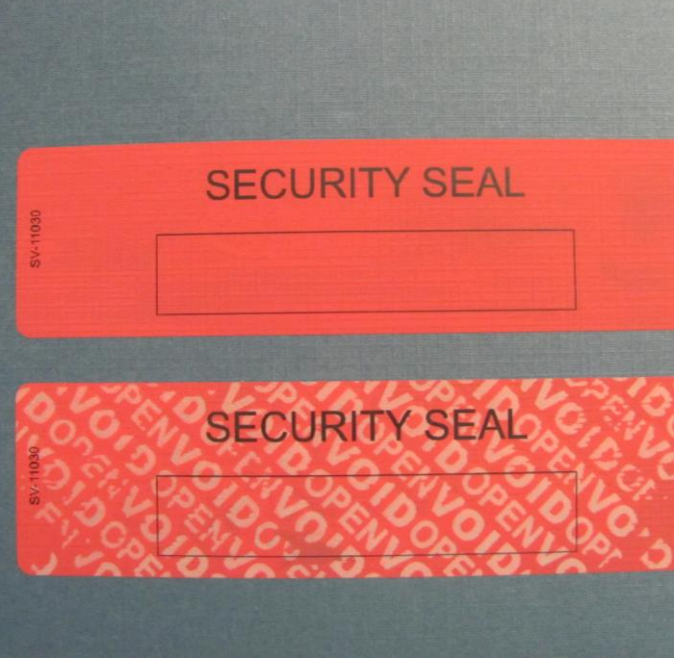
Irradiators

Challenge for inventory control and securing.



Hot Cells

Limited Access.


SECURITY SEAL
SV-11030
SECURITY SEAL
SV-11030


F-127-55X
LOADED
RADIOACTIVE III

Lessons Learned

- Develop a detailed gap analyst for major changes to any regulations.
- Integration of Nuclear Material and Sealed Source.
- Work closely with the Regulator.
- Develop education program for all Custodians of sealed sources.
- Work with specific programs such as Radiation Protection, Transportation, Logistics.