# SECURITY OF RADIOACTIVE SOURCES USED IN INDUSTRIAL RADIATION PROCESSING

**A Joint**
**WINS & International Irradiation Association**
**Best Practice Guide**

## Why You Should Read This Guide

Gamma irradiation facilities can be found in more than 50 countries worldwide. They use high activity cobalt-60 radioactive sources to treat a wide range of products and materials. The largest application of gamma irradiation at these facilities is the sterilisation of single-use medical devices such as surgical gloves, syringes, catheters and surgical implants used in surgery, wound care and other medical treatments.

The radiation processing industry, which includes gamma irradiation facilities, is mature, heavily regulated and has an exemplary safety and security record. Nonetheless, radioactive sources used for gamma irradiation do have the potential to cause great harm if they are not properly managed. A security incident resulting from the inadequate or negligent management of radioactive sources would likely affect normal business operations, the reputation of an organisation and the wider irradiation community. An organisation could be held liable for significant damages, lose business and/or the use of its facilities, and suffer direct and indirect costs that could constitute a serious crisis for the organisation.

Operators of gamma irradiation facilities range from multinational organisations with multiple sites to small organisations with a single facility. These organisations operate under varying legal and regulatory frameworks and have their own internal arrangements and procedures. Meanwhile, the threats, such as from terrorism and cyberattack, have evolved in recent years, and it is important that security arrangements are assessed and updated on a regular basis. Therefore, there is an opportunity and need for the radiation processing industry to take note of international best practice and operational experience.

This joint WINS and International Irradiation Association (iia) Best Practice Guide has been developed to provide a reference that supplements international recommendations and enhances security requirements prescribed by national regulation for gamma irradiation facilities.

The guide aims to help you—as a business leader, radiation safety officer, security specialist, radioactive source user or other stakeholder with responsibility for the management or security of gamma irradiation facilities —understand and manage the security risk. It aims to define the threat and responsibilities of the various stakeholders, provide practical advice on physical protection systems and security management, discuss the importance of security culture and take a whole-life approach towards radioactive sources that includes planning for their end-of-life management.

The overall objective of this guide is to provide gamma irradiation facility operators with best security practices that result in the most effective and efficient security arrangements at their facilities. However, it is meant as a starting point only. Whilst it introduces the subject of source security and gives some industry-specific examples, it is important that security systems are developed taking individual circumstances and the risk environment into account. We recommend reading the additional documents that are referenced, enrolling in the WINS Academy module titled *Radioactive Source Security Management*, and considering joining the International Irradiation Association to become an engaged and informed member of the irradiation community.

### About the Appendices

Appendix A provides a set of questions that stakeholders at all levels of the organisation can use to help determine how effective their current security arrangements are for protecting their organisation's sources. Appendix B defines five different levels of organisational achievement for the security of high activity radioactive sources. Benchmarking where your organisation falls on this scale will help you identify possible gaps in your security infrastructure and provide you with a starting point for improvement.

### About the Preparation of this Guide

The information presented here is based on accepted international guidance and the real-life experiences of security practitioners and managers of gamma irradiation facilities. In particular, WINS and iia would like to thank the following organisations that contributed to the preparation of this guide:

- Gamma-Service Recycling GmbH
- Nordion (Canada) Inc.
- SQHL (Beijing SanQiangHeLi) Radiation Engineering Technology Co., Ltd
- Sterigenics U.S., LLC
- STERIS Applied Sterilization Technologies, STERIS plc
- Symec Engineers (India) Pvt. Ltd.
- VINCA Institute of Nuclear Sciences, University of Belgrade

The International Irradiation Association believes that this joint publication contributes to enhanced understanding of best practice in radiation processing.  The Association endorses this Best Practice Guide and believes that it contributes to the safe and beneficial application of irradiation technology.

This guide also reflects discussions and conclusions from a series of WINS International Best Practice Workshops on the security of radioactive sources that have been held in locations throughout the world.

Wherever possible, this guide uses the same terminology as that found in the International Atomic Energy Agency (IAEA) Nuclear Security Series and Safety Series publications. The preparation of the guide was supported by the US Department of Energy/ National Nuclear Security Administration under Award Number DE-NA0003949.

## We Welcome Your Comments

We periodically update the information in this guide to reflect best practices and new ideas. Therefore, we ask that you read it carefully and then let us know how it can be improved. If you need assistance with any aspect of this guide, please email us. You can also contact us via your WINS membership portal.

**Dr Roger Howsley**
*Executive Director*
*World Institute for Nuclear Security*

March 2020

| WINS Contact Information |
| --- |
| **World Institute for Nuclear Security**<br>Landstrasser Hauptstrasse 1/18<br>AT-1030 Vienna, Austria<br>Email: info@wins.org<br>www.wins.org |

**Mr Paul Wynne**
*Chairman*
*International Irradiation Association*

March 2020

| iia Contact Information |
| --- |
| **International Irradiation Association**<br>4 The Business Plaza, Owen Way,<br>Leominster Enterprise Park, Leominster<br>HR6 0LA, United Kingdom<br>Email: info@iiaglobal.com<br>www.iiaglobal.com |

Version 1.0
ISBN: 978-3-903191-61-7
WINS (20)09

# CONTENTS

## THE USE OF COBALT-60 SOURCES IN GAMMA IRRADIATORS

Cobalt-60 is used in radiation processing facilities, specifically gamma irradiators, as the source of radiation for the treatment of material and products. Processing of material and products is done on an industrial scale and for beneficial applications such as sterilisation, microbial reduction, disinfestation and modification of material to improve its performance. Radiation processing is used globally by many industries and for applications that benefit us all every day.

Cobalt-60 is a non-soluble, non-dispersible and non-flammable metal that is specially produced in nuclear reactors. The cobalt-60 is safely removed from the reactors and manufactured into sealed sources that are designed, tested and approved to meet international regulatory standards.

In a gamma irradiator, the cobalt-60 sources are typically positioned in a rack that is located inside a concrete bunker called an irradiation cell. The product to be treated is carried into the irradiation cell by a conveyor system and circulated around the cobalt-60 sources until it has received the specified dose of radiation. When the cobalt-60 sources are not in use, the rack is lowered into a pool of water for safe storage. A very small number of irradiators do not have a storage pool, in which case the sources are lowered into a shielded pit for safe storage.

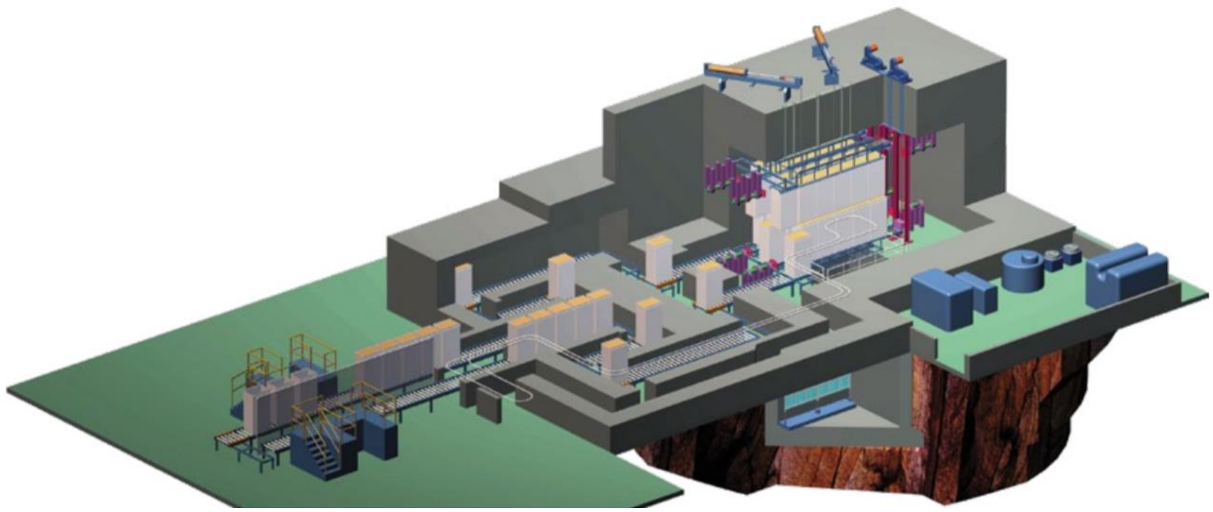


Figure 1: *A typical gamma irradiator for radiation processing. This cut away illustration shows the irradiation cell, conveyor system and storage pool. Illustration of type JS1000 irradiator courtesy of Nordion (Canada) Inc.*

A gamma irradiator used for radiation processing will typically contain from 0.1 to 5 MCi of cobalt-60 made up of many—often several hundred—sources. These sources are defined in the IAEA Safety Guide No. RG-G-1.9 as Category 1 with the following risk in being close to an individual source:

| | |
|---|---|
| Cat 1. | This source, if not safely managed or securely protected, would be likely to cause permanent injury to a person who handled it or who was otherwise in contact with it for more than a few minutes. It would probably be fatal to be close to this amount of unshielded radioactive material for a period in the range of a few minutes to an hour. |

The joint iia-GIPA White Paper "A Comparison of Gamma, E-beam, X-ray and Ethylene Oxide Technologies for the Industrial Sterilization of Medical Devices and Healthcare Products" (August 31, 2017) states that more than 200 large-scale commercial gamma irradiators are in operation in about 50 countries, utilizing some 400 million Curies (Ci) of cobalt-60. In addition, there are smaller gamma irradiators of the same or similar design that are used on a semi-commercial basis or for research.

Figure 2: *A source rack loaded with multiple cobalt-60 sources within the storage pool of a radiation processing facility. Illustration courtesy of STERIS AST.*

# WHY SECURITY IS NEEDED

## The Risk of a Malicious Act

The IAEA, States, regulatory bodies, operators, first responders and other stakeholders are concerned that one or more adversaries might attempt to steal radioactive sources or sabotage the facilities where they are located.

In NSS No. 9, the IAEA explains that a **malicious act** is:

*A deliberate act to remove radioactive material from authorised control (theft) or an act directed against radioactive material (sabotage) that could endanger staff, the public and the environment by exposure to radiation or the release or dispersal of radioactive materials, including the deliberate dispersion of radioactive material to cause economic and social disruption.*

Millions of radioactive sources have been distributed worldwide over the past 50 years, and hundreds of thousands are currently being produced, used and stored. Despite hundreds of these radioactive sources going out of regulatory control (i.e. they can no longer be accounted for), there has never been a radiological dispersal device (dirty bomb) exploded anywhere in the world. It is nevertheless conceivable that radioactive sources could be used maliciously to try and cause harm.

A security incident resulting from the inadequate or negligent management of radioactive sources would likely affect normal business operations and the reputation of an organisation. The organisation could be held liable for psychological trauma stemming from the incident, as well as for any physical damages. Ultimately, financial losses (loss of the use of facilities, lost business, lost wages, recovery costs, replacement costs, clean-up costs, and medical costs for employees and members of the public) could constitute a serious crisis for the organisation.

Gamma irradiators use a large number of high activity cobalt-60 sources, so operators must consider the potential consequences of malicious use of these Category 1 sources. They need to maintain facilities and systems that provide an appropriate level of security.

Gamma irradiators are permanent structures, not portable or mobile, and have an inherent level of protection as a result of their substantial irradiation cell with features to prevent unauthorised access. However, opportunities for additional measures exist and are discussed in this guide.

Additionally, some gamma irradiators are highly automated, so operators must consider any impact on security of having a small number or no staff at all on site. Security arrangements must also take into account activities outside of normal operation, such as when sources are being delivered and installed in the irradiator.

Finally, although the theft of the entire cobalt-60 inventory of a gamma irradiator (up to millions of Curies) would be of extremely high concern, from a risk management perspective, the most likely scenarios to consider would probably be the theft of a single source or a small number of sources.

## Note on Self-Protection

It was long assumed that gamma irradiators are self-protecting due to the very high level of radiation dose (potentially lethal) that would result from exposure to the cobalt-60 sources. However, to fully self-protect, the dose must be sufficient to incapacitate an adversary **before** a malicious act is completed. It is important to recognise that exposure to a high radiation dose may not result in immediate incapacity, allowing time for an adversary or group of individuals to complete a malicious act. Indeed, some adversaries are willing to sacrifice their own life in order to perform a malicious act.

# UNDERSTANDING THE THREAT

## Definition of Terms

In security, an **adversary** is an individual who performs—or attempts to perform—a malicious act. Adversaries can either come from outside the organisation or from within it. **Insiders** are individuals (such as employees, contractors and suppliers) who have authorised access to a facility, transport operation, sensitive information, or computer and communications system who use their trusted position for unauthorised purposes. **Unauthorised purposes** can range from a conventional crime, such as financial fraud, to the sabotage and theft of radioactive material.

> An adversary is also referred to as a **threat**. The IAEA (NSS No. 13) defines a **threat** as:
>
> *A person or group of persons with **motivation**, **intention** and **capability** to commit a malicious act.*

## Intention, Motivation and Capability

As stated in the definition above, threats (adversaries) must have intention, motivation and capability to successfully carry out a malicious act. **Intentions** can be numerous and varied, such as publicity for a cause, disruption of the society, actual harm to one or more individuals, or loss of confidence in the government.

Adversaries' **motivation** for carrying out a malicious act must be strong enough to overcome the barriers to achieving their intention. Adversaries may have different motivations for their malicious activities. Examples of possible motivations include financial or ideological factors, revenge or ego, and coercion.

Furthermore, adversaries must have the **capability** to carry out the act. Adversaries may be highly motivated and have the intent to succeed, but if they do not have the ability to plan their operation, lack the financing and weapons to carry out their plan, or lack the technical skill to use the source for a malicious purpose once they've obtained it, they will fail.

## Credible Threats

Potential adversaries can come from many different avenues and have widely varying motivations. Some examples include:

| | |
|---|---|
| **Common Thieves** | Many incidents involving radioactive sources have been perpetrated by individuals who intended only to steal a vehicle or obtain scrap metal to sell and were completely unaware of what the cargo or metal source actually contained. Compared to some adversaries, they are a relatively low-level threat. |
| **Activists** | Activists are committed to a cause, such as eliminating nuclear power or saving the environment. Many are willing to take certain illegal actions to achieve political or social change, but they seldom intend to harm others and are not usually armed. Therefore, they are considered a low- to medium-level threat. |

| | |
|---|---|
| **Organised Crime** | Organised crime can be defined as 'serious crime that is planned, coordinated, and conducted by people working together on a continuing basis'. Their motivation is often, but not always, financial gain. Although much of the discussion revolves around the consequences that could result from terrorist acts, criminals have also attempted to use radioactive material for malicious purposes. |
| **Terrorists** | States around the world have become increasingly concerned that a non-state actor or terrorist group could acquire a radioactive source to use as a weapon. The source could be acquired through theft from a licensed user, illicit purchase, or even the discovery of an orphaned source (i.e. a source outside of regulatory control). Authorities know that both Islamic State and Al Qaeda have sought to obtain radioactive materials for malicious purposes and are willing to invest a significant amount of time and money to achieve their objective. |

## Insider Threats

Insiders are particularly dangerous because they could use their access, authority and knowledge of a facility to bypass dedicated physical protection, safety measures and operating procedures. They would also have more time to select vulnerable targets and carry out a malicious act. For example, they could tamper with safety equipment to prepare for an act of sabotage. Insiders do not fit a typical profile. They can be any age or sex and could be from any level within an organisation.

The threat can be especially strong if insiders and external adversaries work together to achieve their malicious intentions.

Similar to external threats, insiders can have numerous motivations. Some may have applied for a job at a particular organisation with the intention to carry out a malicious act from the beginning. (In other words, they act as *moles*.) Many insiders had no intention of creating harm when they were first hired, but over time they change. Some may adopt radical political or religious beliefs; some may be experiencing personal issues such as divorce, drug and alcohol addictions; or they could be under financial stresses or subject to some form of extortion.

One of the most common motivators is a feeling of disgruntlement. The Software Engineering Institute (2013) studied computer-related incidents perpetrated by insiders who had sabotaged some aspect of an organisation and/or harmed a specific individual and found that in 92% of the cases, a specific series of events had triggered their actions. Examples of this could include a negative performance appraisal felt to be unfair, not receiving an expected promotion, personal financial issues, being forced into retirement, losing a job unexpectedly through no fault of their own (as when downsizing occurs), and resentment toward senior management.

## Cyber Threats

An evolving challenge for the radiation processing industry, as well as most other businesses, is security's increasing reliance on digital technology at every level. For example, many elements of the physical protection system now rely on digital technologies and the associated IT infrastructures, from operations and communications to alarm monitoring stations, intrusion detection and access control. If not properly protected, these elements are vulnerable to cyberattacks that could degrade system performance.

Another challenge is that operators may store a variety of sensitive information on IT systems that could compromise source security. This may include information relating to: security and emergency response plans; source inventory and technical data; irradiator schematics and designs; access and alarm codes; and transport timing and routes. Such information requires protection against unauthorised disclosure.

Gamma irradiation facility operators may also possess sensitive business data and customer-related materials whose disclosure may have a negative impact on their business.

Cyber threats can be perpetrated by lone individuals, loosely organised groups, active terrorist organisations or nation-states. Such individuals may be external to the organisation, an insider, or a combination of the two. Attacks can occur remotely, from anywhere in the world, and be very difficult to track to their source. Furthermore, cyber weapons are reconfigurable, rapidly diversifiable and continuously evolving.

To put this issue into perspective, Symantec (2019) analyses the trends and types of attacks that take place each year, and they continue to increase significantly. In its 2019 report, Symantec says it records events from 123 million attack sensors worldwide, blocks 142 million threats **daily**, and monitors threat activities in more than 157 countries. The cyber landscape becomes more challenging every year, with challenges such as the growing Internet of Things, malicious file attachments that execute a malware script as soon as a document is opened, and high risk apps that are installed on mobile devices.

Clearly, cyberattacks pose a threat to radiation processing organisations, as well as to all other industries and businesses, both large and small. The following is just one example.

> Ashford (2017), writing in *Computer Weekly*, reports that a security researcher (Ruben Santamarta) has discovered numerous security flaws in multiple devices that are used to detect radiation in critical facilities, including hospitals. In one experiment, Santamarta reverse engineered the firmware used in a radiation monitoring gate and was able to find a backdoor password that would have enabled him to bypass the authentication processes and take control of the device so that it would not trigger an alarm.

For all of these reasons, it is imperative that all stakeholders clearly understand the potential threats and work closely together to defend against them.

## Questions for Reflection

- Do you believe your organisation faces threats from any of the adversaries identified above?
- Are you aware of any security incidents at your or other gamma irradiation facilities?
- How often are you briefed on credible threats to your facility? Do these briefings cover threats to radioactive sources?
- How well prepared are you to respond adequately to an incident involving outside adversaries? Insiders? A combination of both?

# ROLES AND RESPONSIBILITIES FOR RADIOACTIVE SOURCE SECURITY AT GAMMA IRRADIATION FACILITIES

Numerous stakeholders, in particular the international community, States, their national regulators and licensees (gamma irradiator operators), are involved in the effort to strengthen radioactive source security both domestically and around the world. Ensuring effective radiological security requires first that all stakeholders and individuals understand and carry out their respective responsibilities effectively.

## The International Framework

The international community is responsible for developing initiatives and instruments that help strengthen nuclear security in States and increase international cooperation. Some of the most important international instruments have been developed by the IAEA; others have been initiated by the United Nations and individual States. These instruments contain both binding and non-binding legal obligations and recognise the important role of the IAEA in helping States meet their obligations and commitments.

### The IAEA

The International Atomic Energy Agency, which is based in Vienna, Austria, is the leading international organisation for the promotion of the safe, secure and peaceful use of nuclear energy, science and technology. Most countries in the world are members of the IAEA. These member states work together to produce international recommendations and guidance that is implemented primarily by governments and regulatory bodies. Governments and regulators frequently use this guidance (which is non-binding) to design their own policies and regulatory arrangements at the national level.

#### The Code of Conduct on the Safety and Security of Radioactive Sources

The most important IAEA document for those with responsibilities for the security of radioactive sources is the Code of Conduct on the Safety and Security of Radioactive Sources. First implemented in 2001, the Code describes how States can safely and securely manage high risk radioactive sources. Following the terror attacks in the US of 11 September 2001, the international community came together to revise the Code. The revised version, which was published in 2004, marked the beginning of a global trend towards the increased control of, accounting for, and security of radioactive sources. This Code currently has two supplementary guidance documents: Guidance on the Import and Export of Radioactive Sources and Guidance on the Management of Disused Radioactive Sources.

**The Nuclear Security Series Publications**

The IAEA publishes the Nuclear Security Series (NSS) of documents. Agreed by IAEA Member States, these documents provide recommendations and guidance for how States can voluntarily enhance their regulatory systems to ensure an effective regime for the security of nuclear and other radioactive materials. The series comprises four sets of publications:

**Nuclear Security Fundamentals**, which describe the fundamental objective and essential elements of a State's national nuclear security regime.

**Recommendations**, which set out measures that States could take to achieve and maintain an effective regime.

**Implementing Guides**, which provide guidance on how States can implement the recommendations.

**Technical Guidance**, which provide more detailed guidance on specific methodologies and techniques for implementing security measures.

The NSS documents cover a range of nuclear and radioactive materials, facilities and topics. Those publications that are most relevant to the security of radiation processing facilities, in particular NSS 11, are detailed in "Suggestions for Further Reading".

## World Institute for Nuclear Security

The World Institute for Nuclear Security (WINS) was established in late 2008 as a non-governmental membership organisation tasked with filling a perceived gap in the nuclear security architecture: creating a forum in which best security management practices could be identified, learned and shared. WINS has held over 120 International Best Practice Workshops all over the world and published numerous Best Practice Guides on a wide range of security management issues. All WINS guides take the perspective of the operator and address issues that have been raised by WINS members, such as challenges surrounding implementation. Those Guides that are most relevant to the security of radiation processing facilities, are detailed in "Suggestions for Further Reading".

WINS launched the WINS Academy in 2014 to help develop demonstrable competence in nuclear security management through training and certification. The programme centres on a core philosophy that presents security as a strategic activity that should be implemented across an organisation as a fundamental aspect of risk management and corporate reputation. In February 2020, WINS established a standalone certification programme for radioactive source security management. This programme is for anyone who has responsibilities for managing the security of radioactive sources. This could include leaders and managers of healthcare facilities, industrial irradiation, well logging or radiography operations, research institutes, or even law enforcement agencies who want to enhance their knowledge about radioactive source security.

### The International Irradiation Association

The International Irradiation Association (iia) was established in 2004 and is a recognised NGO of the IAEA. It represents the industrial irradiation community that includes gamma, electron beam and X-ray technologies. A core aim of the iia is to promote the safe and beneficial use of irradiation technologies. Members include a diverse array of organisations with an interest in the scientific and commercial application of the technology. Members of iia include manufacturers, producers and suppliers of cobalt-60 and electron beam/X-ray technology, multinational and national radiation processing facility operators, universities, institutes and organisations providing support services. The membership is geographically diverse and provides a basis for network and collaboration.

The iia has links via affiliated and connected organisations to many countries and to the development and oversight of industry best practice. It assists in the drafting of documents, white papers and reports and prepares white papers and reference material for its members and the wider irradiation community.

## State Roles & Responsibilities

Ultimate responsibility for radioactive source security rests with individual States. The State's first responsibility in this regard is to establish, implement and maintain the overall **framework** for regulating the security of nuclear and other radioactive material. This requires States to enact national laws, regulations and codes that assign responsibility, actions, goals and requirements.

The State is also responsible for creating one or more independent **regulatory bodies** with the required resources—technical, human and financial—to regulate nuclear and other radioactive material. The regulatory body should have a clearly defined legal status; be completely independent from operators; and have the legal authority, competence and financial and human resources necessary to perform its responsibilities and functions effectively.

### The National Threat Assessment

It is the State's responsibility to perform a **national threat assessment** that identifies the motivations, intentions and capabilities of possible adversaries; the likelihood that certain malicious acts will occur; and the potential consequences that could occur if an incident should take place. The outcomes of the national threat assessment are used for identifying a set of credible threats that allow regulators to develop requirements capable of mitigating these threats or operators to directly design effective security arrangements for their radioactive sources.

The inputs to a threat assessment and its outputs are likely to be sensitive (i.e. classified) because they include data obtained from intelligence and law enforcement agencies about the actual threats known to exist within the State or those that could credibly materialise. Because of its highly sensitive nature, the raw intelligence is not generally divulged to operators. However, operators may have crucial information about their location and facilities that should be included in the assessment, so ideally, they will be consulted in the process.

## Regulatory Body Roles & Responsibilities

It is the responsibility of the regulatory body for radioactive sources to establish regulations and requirements that operators must fulfil to ensure the safety and security of the radioactive sources under their control. These regulations can be benchmarked against the provisions contained in the Code of Conduct for the Safety and Security of Radioactive Sources, as well as in IAEA NSS No. 14 (*Nuclear Security Recommendations on Radioactive Material and Associated Facilities*), No. 11 (*Security of Radioactive Sources*), and No. 9 (*Security in the Transport of Radioactive Material*).

### Regulatory Approaches

When it comes to regulating operators, regulatory bodies can take three basic approaches: prescriptive, performance-based, or a combination of the two. In a **prescriptive** approach, the regulator specifies all of the measures an operator must implement to meet the security goals and objectives, and the operator simply obeys. In a **performance-based** approach, the regulator determines the overall goals and objectives and requires operators to design a security system that demonstrably meets them. In the **combined** approach, the regulator draws on aspects of both the prescriptive and performance-based approaches.

Each approach has benefits and drawbacks. For example, the prescriptive approach tends to be the most economical and requires less expertise from the operator. However, this also means that the operator has very little impact on regulatory decision making. It also means there can be a tendency to implement only the security measures that are required and nothing more.

The performance-based approach encourages operators to take a more proactive approach to security and gives them much more flexibility when it comes to designing their security systems. In addition, it encourages better communication between the regulatory body and operators. On the other hand, it also requires greater expertise on the part of the operator and can be challenging to implement, but the objective is to fully integrate security into an organisation's risk management policies and practices.

Regardless of which approach is taken, it is important for operators to realise that just because they comply with all regulations, their security system may still not be effective. They need to conduct their own risk analyses and implement additional security measures if the situation warrants it.

### The Operator-Regulatory Body Relationship

It is important for operators and the regulatory body to develop a relationship with each other that enables communication to flow back and forth between them. Although it is operators' responsibility to comply with all regulations, they should also be able to provide input during the regulatory development process. For example, if a new regulation will place undue financial burden on operators, they may be able to suggest a different, less costly approach that would lead to similarly effective results. This is one benefit of performance-based regulation.

## Operator Roles and Responsibilities

Operators have the primary responsibility for designing, implementing and maintaining security systems for radioactive material in accordance with the regulatory requirements in their State and any other further security objectives defined by the organisation itself. To ensure that no undue risk to the health of individuals; to reputation, brand and business continuity; or public confidence occurs, an organisation must establish and maintain the requisite financial, human and technical resources necessary to achieve effective security in a way that supports the organisation's operational and business objectives.

It is the operator's responsibility to remedy any non-compliances identified by the regulatory body, investigate the issue according to an agreed time schedule, and take any necessary actions to prevent recurrence. (In turn the regulator needs to verify that the operator has implemented the remedial actions effectively.)

### A Risk-Informed Approach

Operators should use a risk-informed approach to manage the security of their radioactive sources. This begins with the awareness that security is a corporate-wide responsibility, similar to safety, in which all of the operator's stakeholders have responsibilities. A risk-informed approach requires that operators regularly assess the risks; develop, evaluate and implement mitigation measures; and monitor and manage the resulting actions for relevance and effectiveness. Such a process helps organisations allocate their resources more effectively and efficiently.

### Leadership

The board (or equivalent) and executive management play a crucial role in their organisation's safety and security because they set the policies, decide on the corporate risk appetite, allocate funding, and ensure that policies and programmes are developed and implemented.

If leadership fails to carry out its responsibilities effectively and an incident occurs, the consequences for individuals, communities and the environment—as well as for the organisation's financial stability, reputation and liability—could be significant.

In addition, security culture begins at the top and filters from there throughout the rest of the organisation. This is why leaders' first responsibility is to lead by example. They must clearly demonstrate their belief that a credible threat exists and that security of radioactive material is important by following all security-related policies and procedures themselves and by treating security as a business risk similar to safety.

**Leadership responsibilities for radioactive source security include:**

- Establish clear expectations, accountabilities and policies for security for all management and staff.
- Systematically communicate their security priorities.
- Encourage teamwork and cooperation.
- Establish mechanisms to promote behaviour that supports security, such as encouraging staff to raise concerns and make suggestions for improvement.
- Develop tools and methodologies with which to regularly assess the security culture within the organisation.
- Ensure that all personnel have the skills, knowledge and authorisations they need to carry out their security responsibilities.

## The Security Policy

The security policy lays the foundation for the management systems that ensure the security of an organisation's radioactive sources. It is the responsibility of the board (or similar body) to create a well-defined policy that demonstrates the organisation's commitment to high quality performance in all of its nuclear security activities. This begins by giving security a high priority, similar to other business risks. Leadership should also provide the necessary financial, technical and human resources to carry out all of the organisation's security responsibilities. This includes appointing a specific individual with the authority, autonomy and resources to implement and manage security activities. The policy should be in a clear, written format and provided to all staff.

## The Security Plan

An effective security plan documents the design, operation and maintenance of the entire security system. It defines the design requirements, documents regulatory compliance, and directs the implementation of the policies and procedures for operation of the security system to ensure all defined security objectives are met.

Usually no single document can consolidate all security related information. The security plan is the central piece of the security documentation and needs to be structured around key areas and refer to lower level documentation that can be reviewed independently and in some cases be compartmentalised to reduce the risk that the plan is lost or compromised.

Every permanent or temporary site where cobalt-60 sources are used or stored should have a security plan specific to that location. Furthermore, the security plan should include all information necessary to describe the security approach and the systems used to protect sources. Because such information is sensitive, it needs to be protected and made available only to authorised individuals with a need to know.

To be operationally effective, the security plan should be routinely reviewed, evaluated and updated. Committing to such actions also helps to instil and promote a strong security culture because it stimulates periodic review and rehearsal of security arrangements.

**Key areas to be covered by the security plan and associated documents**

SECURITY REQUIREMENTS AND OBJECTIVES

- Regulatory Requirements
- Other Security Requirements
- Objective of the Security Plan
- Preparing and Updating the Security Plan

This section provides an overview of the requirements for preparing the security plan, the plan's objective and scope, and a description of how the security plan was prepared and how it will be periodically reviewed and updated.

FACILITY DESCRIPTION

- Overview
- Radioactive Material
- Categorisation and Security Level
- Physical Description
- Operational Description
- Regulatory Requirements

The facility description provides an overview of the facility mission, a description of the cobalt-60 present, its categorisation and security level, and the physical and operational aspects of the facility.

SECURITY MANAGEMENT

- Roles and Responsibilities
- Training and Qualification
- Access Authorisation
- Trustworthiness
- Information Protection
- Maintenance Programme
- Budget and Resource Planning
- Evaluation for Compliance and Effectiveness

The security management section explains how security management is being implemented. This includes a description of the security roles and responsibilities, how access authorisation is assigned, and the methods used to assess personnel trustworthiness. It also describes how personnel are trained in security, what their qualifications are, how budgets and resources are planned, how sensitive information is protected, and the methods used to regularly evaluate system performance and compliance.

SECURITY SYSTEM

- Security Assessment Methodology
- Threat Information
- Security System Design
- Access Control
- Deter, Detect and Assess, Delay, Respond
- Internal and External Audit, Testing and Assessment of System

The security system section describes the security assessment methodology, how threat information is used to design the security system and the overall security system design. It also provides details on all equipment and procedures put in place to perform the security functions.

SECURITY PROCEDURES

- Routine, Non-Routine and Emergency Operations
- Opening and Closing of Facility
- Key and Lock Control
- Accounting and Inventory
- Acceptance and Transfer

This section outlines the procedures for routine, non-routine (e.g. instances of source installation) and emergency operation of the security system, opening and closing of the facility, key and lock control, accounting and inventory, and acceptance and transfer.

RESPONSE

- Security Events and other Situations of Security Concern
- Communications
- Security Event Reporting
- Security during Emergencies and Contingencies
- Increased Threat Level

The response section includes a description of the response to security events, communications, security event reporting, security during emergencies and contingencies, and measures to address increased threat levels.

CYBERSECURITY

- Cyber threats
- Potential cyber vulnerabilities of the security system
- Cybersecurity measures
- Procedures in case of cyber incident

The cybersecurity section includes a description of the digital components of the security system, the roles and responsibilities for cybersecurity, the preventive cybersecurity measures, functionality and performance testing procedures, and response arrangements and temporary measures in case of a cyber incident affecting the security system.

## Questions for Reflection

- Which approach to regulating radioactive sources does your regulatory body take? What do you think the benefits and drawbacks of this approach are for your organisation?
- How would you rate the relationship between operators and the regulator in your country? If needed, would you have suggestions for improving this relationship?
- How satisfied are you with the understanding and engagement of your senior management in radioactive source security matters?

# EFFECTIVE PHYSICAL PROTECTION SYSTEMS & SECURITY MANAGEMENT

To ensure the security of their cobalt-60 sources, operators need to implement a security system based upon the functions of deterrence, detection, delay and response. They also need to take a graded approach to security and ensure that their system provides defence in depth. In addition to these technical measures, operators need to implement security management measures that address such issues as trustworthiness, staff training, information protection, inventory control and incident response and reporting.

## Physical Protection Functions (Deter, Detect, Delay, Respond)

Physical protection has four functions that form the basis of the security system. The first is to **deter** adversaries from even attempting to steal or sabotage radioactive sources. The second is to **detect** and **assess** any attempts that adversaries might be making. The third and fourth are to **delay** adversaries who are attempting to steal or sabotage sources until an adequate **response** force (e.g. the police) can arrive and interrupt or neutralise them. Each of these functions is important and works with the others to achieve an effective security system.


In order to ensure that the response time is less than the time required to perform a malicious act, consideration should be given to how: the adversary can be detected and verified as early as possible; delay time can be increased; and response time can be reduced. When designing its security system, the operators should identify credible attack scenarios and implement appropriate delay and detection elements to ensure a timely response.

### Deter

**Deterrence** occurs when an adversary is dissuaded from undertaking a malicious act because the perceived robustness of a site's security systems would make the attempt too difficult to mount, success would be too uncertain, and/or the consequences for themselves would be too unpleasant. Deterrence is a by-product of effective physical protection design and of the security culture of an organisation, not a standalone security measure. Therefore, it should not be assumed that deterrence measures alone will be effective against adversaries who have both capability and motivation.

**Examples for use at gamma irradiation facilities include** perimeter fencing, good lighting, video cameras, signage and, in some cases, the use of security guards. These highly visible measures demonstrate that the facility has multiple layers of robust security in place.

The insider threat can be deterred by the requirement for two people to use multiple authentication methods (e.g. fingerprint and PIN or ID card) to access secure areas. This needs to be supported by a good security culture amongst the staff and the effective implementation of the security procedures.

*Figure 3: CCTV can be highly visible and will contribute to both deterring and detecting an adversary.*

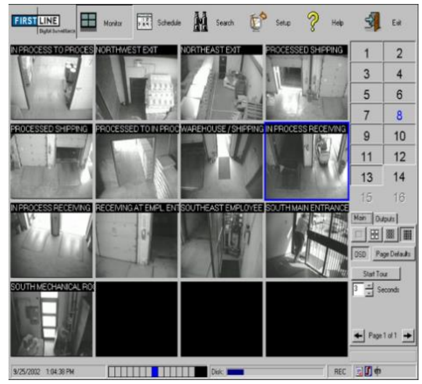



*Figure 4: Multiple zones (personnel entrances, goods and warehouse areas, selected rooms etc.) can be monitored at one time. Courtesy of STERIS AST.*

## Detect (and Assess)

**Detection** is the discovery of an intrusion, an attempt to steal or sabotage radioactive material or any other unauthorised action. Detection measures are intended to create an alert should adversaries attempt to enter an area they are unauthorised to access or to perform an unauthorised action.

**Examples for use at gamma irradiation facilities include:**

- **Access control:** The objective of access control is to ensure that only approved individuals with a need to access certain areas of the facility or the irradiator have access to them. Access can be controlled by a key, an electronic card (e.g. magnetic swipe or proximity pass), PIN code entry or biometric reader. Ideally, an access control system should combine at least two of these measures. Access can be zoned so, for example, all staff have access to the building but only specifically qualified and approved staff can access the irradiator. Systems should enable temporary security zones for periods of irradiation shutdown when work such as maintenance and source handing may be required. Whenever possible, it is good practice to track and record access to the different zones.
- **Intruder detection and alarm:** Intruder detection systems should be designed so that detection is assured for all feasible paths leading to the gamma irradiator. Detection systems may include motion detectors, door contacts, floor sensors and glass break detectors. Every alarm signal should be reported on-site and off-site, and alarms should be monitored 24 hours a day, seven days a week. It is good practice to categorise and prioritise alarms in order to develop specific response procedures, should the alarm happen for instance in a warehouse or at the door of the irradiation cell.
- **Video/CCTV:** If an alarm should go off, it must be **assessed** immediately to determine whether the alarm indicates an actual security event or some form of harmless anomaly. This assessment can be made either by an individual at the location of the alarm or remotely through CCTV and other monitoring systems. Detection without assessment has no value because until an event is detected and verified to be a real security incident, no response will take place.

- **Radiation Detection:** The use of radiation monitors at points of access can provide early detection of the unauthorised removal of a radioactive source. This detection can be alarmed both internally and externally and can be assessed using video/CCTV.
- **Employee Security Awareness Training:** Initial and periodic training on the types of suspicious activity will make employees more aware of security and able to report suspicious activity for assessment.

*Figure 5: (Courtesy of Symec Engineers)*


*Figure 6: (Courtesy of VINCA Institute)*

*Various methods of controlling access are available to operators of irradiation facilities. These include turnstiles and PIN code keypads, as illustrated above.*

## Delay

**Delay** follows detection. Measures consist of physical barriers with the purpose of increasing the time it would take adversaries to successfully remove cobalt-60 sources from a facility or carry out an act of sabotage. Multiple layers that create delays can be most effective because the longer adversaries can be delayed, the greater the chance that an effective response can be mobilised in time to interrupt them. Delay mechanisms that may compromise safety must not be introduced.

**Examples for use at gamma irradiation facilities include:**

- **Heavy-duty doors:** Metal security-rated doors that are secured into robust frames and walls can cause significant delay to unauthorised access, particularly when used in conjunction with high-security locks/interlocks. They should be installed where direct access to the irradiation cell or other sensitive/controlled areas is possible.
- **Source storage pool barriers**: These items can prevent direct access to the rack that holds the cobalt-60 sources. A pool cover of hardened design will prevent access when the source rack is lowered. A source rack shroud may delay access to a raised rack depending on its design, although a raised rack is of less concern as the radiation level will impair an attackers ability to access the cobalt-60 sources. These items can incorporate security fittings that require specialist tools for removal.

- **Secure tools:** Any tools that could aid an intruder should be locked away when not in use. Special attention should be given to source handling tools, which should be stored in a secure room when not in use.
- **Roof plug and crane:** If applicable, the cell roof plug should be locked into place during routine operation of the irradiator. Any internal crane that is used solely for removing the roof plug should also be locked or disconnected from power when not in use.
- **Circuitous route:** Delay can be caused by forcing an intruder to use an indirect route between the point of accessing the building and the cobalt-60 sources. If practical, forcing an intruder to pass through offices or multiple doors and features such as internal fencing can be used to achieve this. Consideration must be given to the practicalities of routine radiation processing operations and the flow of product and authorised people through the facility.

*Figure 7: Security door and fencing (Courtesy of Gamma-Service Recycling GmbH)*

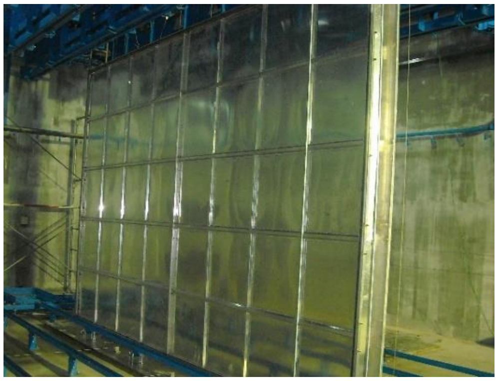


*Figure 8: Source rack shroud (Courtesy of SQHL Radiation Engineering Technology Co., Ltd)*

*Heavy-duty security doors and the use of fencing that causes an intruder to use an indirect route will delay access to secure areas such as the irradiation cell. Depending on its design, a source rack shroud may delay access to the sources.*

### Respond

**Response** refers to the actions undertaken by onsite security forces (if present) and/or offsite law enforcement to interrupt and subdue an adversary while the malicious act is in progress.

Operators of gamma irradiators must assess and respond to any security event in accordance with their security procedures and with a priority for the safety of staff.

Responders need to be properly trained and equipped and have the authority and ability to carry out their assigned actions. They must be familiar with the site, know who is responsible for what, and have the necessary resources to stop the malicious act.

## Graded Approach

Protective measures need to be proportionate to the risk. Knowing how much security is enough is one of the challenges of implementing effective security measures. Too little security may leave sources vulnerable, but too much security wastes money and could unnecessarily impact operations.

To address this issue, regulators and operators should take a **graded approach** toward security. In essence, this means that material with high consequences from malicious use should receive more attention and stricter security measures than material with lower consequences. Category 1 sources, such as the cobalt-60 used in gamma irradiators, need more stringent protection measures than material with lower consequence.

## Defence in Depth

The IAEA (NSS No. 13) defines **defence in depth** as "the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised". Such an approach requires a mixture of hardware, procedures and facility design. This approach means that an adversary has to avoid or defeat a number of different security measures in sequence—such as penetrating multiple separate barriers before gaining access to a source rack—in order to be successful. Defence in depth helps to deter or defeat an adversary because it adds uncertainty, requires different techniques and tools, creates additional hurdles and requires more time.

## Security by Design

The ideal approach to securing cobalt-60 sources is to *design-in* or *engineer-in* the required physical security features when designing a new gamma irradiation facility. Costs can be reduced by incorporating security into the original design rather than retrofitting facilities at a later date.

The **security by design** approach enables operators to identify ways in which safety and security design can work with and enhance each other. For example, the wall thickness of an irradiation cell is an important consideration for radiation safety but can also be an important security feature.

Security by design enables engineers to ensure their design is balanced between detection, delay and response elements, all of which need to work together to ensure security. Design must not impact safety and should have a minimal impact on routine radiation processing operations.

**Examples of security by design of gamma irradiation facilities include:**

- **Security perimeters:** site, warehouse and irradiator perimeters should be designed-in. Within these parameters, **multiple layers** of physical protection are designed-in to be supported by appropriate procedures that enhance security.
- **Access to the irradiator cell** should incorporate hardening, intrusion detection and radiation detection at the personnel and product entry and exit points.
- **The source storage pool** can incorporate a secured cover that blocks access to the source rack when the rack is in the lowered position.  These covers should be of hardened design so resistant to a variety of tools and incorporate security fittings so they are not easily removable by attackers.
- **The source rack and modules** should incorporate locking features.
- **Independent systems:** Computer-based security systems should be independent from the irradiator operating system wherever possible, whilst recognising that some interface between the systems is necessary. This can reduce the risk of unauthorised access or overriding one system via the other system.


*Figure 9: Access to the irradiator cell should be via a hardened security door fitted with opening detection sensors. Security can work hand in hand with safety, for example by interlocking a mechanical latch bar with the mechanism for lowering the source rack into a safe position as shown. The security of this mechanism, including encasement and tamper detection, should be considered. Illustration courtesy of Symec Engineers.*

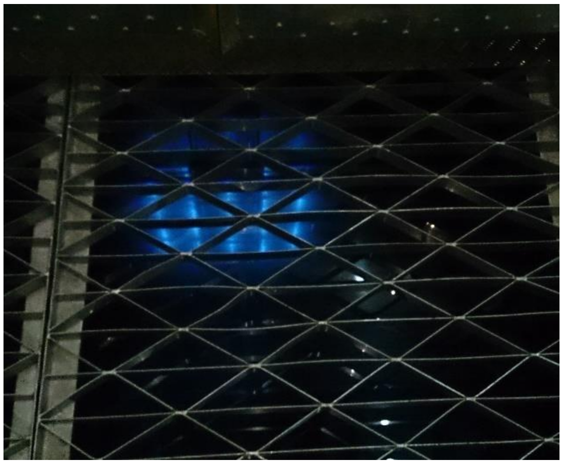


*Figure 10: Access to the sources within the irradiator will be delayed by use of a pool cover. Various designs of solid covers or grills may be used and, in order to be effective, should be of hardened design, resistant to various tools, incorporate security fittings and not easily removeable by multiple attackers. Illustration courtesy of Symec Engineers.*

## Security during Temporary Operations

Security requirements during temporary operations such as cobalt-60 receipt/dispatch and installation need to be considered and will vary from those during normal irradiator operations.

During cobalt-60 receipt/dispatch, the sources will be inside transport containers, either on or off a vehicle, and there may be need for greater access to the irradiator building for vehicle movements. For example, doors additional to those used to allow the flow of product being processed may be opened to allow the vehicle and transport containers to access the irradiation cell.

During a cobalt-60 source installation, physical barriers such as the pool cover will need to be removed to enable access to the source rack. There will be a greater need to access the irradiation cell via the maze, and the roof plug may be removed for an extended period of time.

Some layers of security will be removed during these temporary operations. It is therefore important to review these operations in detail, understand any temporary vulnerabilities and put additional security in place to mitigate these vulnerabilities. Temporary security measures may include greater coordination with local law enforcement agencies, additional security/response personnel, reduced personnel access to designated areas, temporary physical barriers and a greater level of video surveillance.

Temporary security arrangements must be recorded as procedures within the security plan. Emergency responders must be made aware of these temporary operations and be briefed on how the situation varies from normal irradiator operation so they can plan their modified response accordingly.

## Ensuring the Cybersecurity of Security Systems

Following the global trend in all sectors and activities, security systems components are more and more reliant on digital technologies and associated information technology (IT) infrastructures. These components include operations, communications, alarm monitoring, and fundamental elements of the intrusion detection, access control and alarm assessment systems. If not properly protected, these elements are vulnerable to cyberattacks that could degrade the performance of the PPS and lead to vulnerabilities in the security of the radioactive sources themselves.

The possibility of an adversary attack blending cyber and physical component should be considered by gamma irradiation facility operators and measures to reduce the risk as low as reasonably achievable should be implemented.

Cybersecurity is a specialist area and is not covered in detail in this guide. Operators are encouraged to read the US/DOE/NNSA guidance document on Cybersecurity Best Practices for Users of Radioactive Sources.

Operators should seek advice from experts who will recommend appropriate cyber security measures, including hardware, software, penetration testing and response procedures. When discussing with their IT colleagues or contractors, operators should keep the following in mind:

- IT Systems require maintenance and software must be kept up to date. Firewalls should be tested, software should be patched regularly and unnecessary programs should be removed.
- Security systems should be independent from other irradiator or business systems where possible. This will reduce the risk of an attacker being able to access one system via another.
- Elements of the security system should meet highest industry standards and should include tamper indicating devices to prevent unauthorised access or manipulation.
- The use if IP (Internet Protocol) video cameras offer greater security over analogue cameras. IP cameras make data difficult to intercept as they encrypt and compress data before transporting it over the internet to a server.
- The cyber vulnerability of communicating data to an offsite monitoring station should be assessed. redundant and independent means of communication should be used,
- The removal of unnecessary access ports such as USB drives can reduce the potential for unauthorised access.

## Human Trustworthiness and Reliability

Operators need to know that their staff can be trusted with the sensitive information, critical technology and potentially hazardous materials with which they work. This is why they need to put a human reliability assessment plan in place that carefully vets potential staff before they are allowed access to sensitive information, critical technology or radioactive material. An assessment plan will help to ensure staff remain reliable during their employment and identify procedures to follow when staff terminate their employment.

### Vetting

Because vetting helps to determine the trustworthiness and reliability of potential staff, it is a key measure in mitigating the threat posed by insiders. The process can range from a simple confirmation of identity to a comprehensive background check conducted by the national authority that includes verifying whether the individual has a criminal history or any other ‘red flags’ that might indicate issues of concern.

### Behaviour Observation

It is important to remember that initial vetting does not guarantee future reliability because people’s lives, attitudes and circumstances can change over time. Consequently, the trustworthiness of individuals with access to cobalt-60 sources needs to be re-checked periodically, and any new information affecting an individual’s reliability needs to be brought quickly to the attention of the appropriate authorities. Staff also need to be trained how to report suspicious behaviours, non-compliance with security procedures, and any other security incidents or concerns they might have.

Measures taken to improve human reliability are more effective when organisations emphasise that safety and security are two sides of the same coin. For example, a human reliability issue involving an individual who is drinking alcohol or taking drugs on the job can be a threat to both safety and security. Because staff are the first and potentially only line of defence against insider threats, they need to have access to a clearly defined and easily utilised programme for sharing concerns. If they notice concerning behaviours, they need to know they have a duty to report them and that a programme is in place for doing so. They also need to know that the issue will be investigated thoroughly and promptly and that they will not be penalised for making a report.

### Post-Employment Procedures

Operators need to have written procedures to follow when it comes to the termination of employment. These include such actions as:

- Removing access to sensitive locations, materials and data
- Changing passcodes or combinations
- Removing cyber access
- Collecting all badges, ID cards and parking permits

Special care needs to be taken not to risk the possibility that soon-to-be ex-staff members hear about their termination through unofficial channels while they possess the access, knowledge and authority to impact sensitive operations. A human resources manager needs to hold an exit interview when the employee is informed of this decision, and all of the regular post-employment security steps listed above need to be performed immediately.

## Information Protection

Information that could compromise cobalt-60 source security is sensitive and needs to be protected. This includes information related to the security plan, access codes, alarm system codes/passwords and intimate details of the physical security element. It also includes the cobalt-60 source inventory, operational procedures, computer systems, transport timing and routes (for both cobalt-60 and products for radiation processing), as well as technical data, blueprints, schematics, designs, security procedures and emergency response plans.

Information protection involves the development, implementation and maintenance of written policies and procedures that describe how to handle sensitive information and protect it from unauthorised disclosure. Operators should evaluate an individual's **need to know** before allowing access to security documents. Information protection policies and procedures should include instructions on how to:

- Protect sensitive information about cobalt-60 sources that are in use or transit.
- Prepare, identify, mark and transmit - both physically and electronically - documents or correspondence containing information about the operator's security programme.
- Control access to information about the operator's security programme.
- Destroy or remove documents from the protected information category when they become obsolete or are no longer sensitive.

## Incident Response Planning, Coordination and Reporting

Operators of gamma irradiation facilities need to plan the incident response procedures that should be followed in close coordination with their emergency responders (e.g. police, ambulances and fire departments.) The procedures need to address how to handle both radiation safety and radiation security emergencies. Planning should include temporary situations such during cobalt-60 source delivery, receipt and installation.

If possible, operators should periodically conduct basic radiation safety and security training for the offsite response force.

It is crucial that first responders have a list of the basic contacts at the operator's site and understand:

- The types and quantities of radioactive material and associated devices onsite.
- The potential hazards associated with loss of control of sources.
- Specific facility information (floor plans, entrances, points of egress, etc.)
- Site-specific physical protection measures that the operator uses to monitor premises and delay an adversary from gaining access to the material.

To develop effective coordination, operators need to regularly communicate and periodically meet with their offsite response force. Both entities need to know who the points of contact are at each other's organisations and have their full, up-to-date contact information. In addition, operators need to determine whether their local emergency response force is available day or night, seven days a week, to provide an armed response and arrest perpetrators. If not, they will need to identify and coordinate with the closest response force that can provide such services if the primary response force is off duty.

Operators should report security events to the regulatory body and—depending on the circumstances—to law enforcement as well.

## Questions for Reflection

- When considering your own facility, what kind of measures have been implemented to deter, detect and assess, delay and respond to a security incident? Do you find them adequate?
- Did your organisation carefully vet you when you were first hired? Do you believe the vetting process in your organisation is sufficient for mitigating insider threat?
- Does your organisation have integrated security arrangements that link conventional and radiological security?

# SUSTAINING YOUR SECURITY ARRANGEMENTS

Sustaining cobalt-60 source security entails a great deal more than compliance with the basic physical protection measures and regulations stipulated by the regulatory body. It requires operators to take a proactive approach to security that involves managing the entire lifecycle of their sources from original purchase to final disposal. It also requires taking steps to measure and improve security culture, increase the professional security competence of staff, participate actively in benchmarking and peer review activities, and harmonise security and safety.

## Take a Whole-Life Approach

When creating a budget and planning resources for cobalt-60 source security, it is important to take a whole-life approach (sometimes called *cradle to grave*). This requires operators to plan for and finance the final handling of their cobalt-60 sources when they reach the end of their life.

The radiation processing industry has a good record of handling end-of-life source that are typically returned to their supplier or another authorised operator. These organisations generally have the capacity to safely and securely manage the radioactive sources they provide and are better able to determine whether disused sources can be reused, recycled or relegated to final disposal.

There are certain considerations for operators that plan to return cobalt-60 sources to their supplier or other authorised operator. These will help ensure that the sources can be handled in an effective manner:

- End-of-life of radioactive sources can be handled in multiple ways (e.g. storage, re-use, recycling) and by multiple authorised organisations. Operators should evaluate their options. Timely handling of end-of-life sources can contribute to security as well as operational flexibility and cost efficiency.

- The end-of-life handling of sources requires funding, and it is important that operators have a financial mechanism (financial provision, bond etc.) to cover this cost. Cobalt-60 sources used in radiation processing have a long operational life, typically 20 years, so it is not usually possible for a supplier or other authorised operator to accurately know the final method and cost of end-of-life handling at the time of supply. This is because operational and regulatory changes are likely to occur over the life of the source as well as direct cost changes. It is therefore important that operators, in coordination with source suppliers, update their plans periodically with current costs and adjust their financial arrangements accordingly.
- The return of sources to suppliers is often on a 'one for one' basis (i.e. one end-of-life source can be returned to supplier for each new source supplied). It is important for operators to recognize that different costs may apply for sources that are returned outside of this basis, for example, if a gamma irradiator is being decommissioned and all sources require removal and handling.
- Sources in temporary storage within an irradiator are subject to the same security requirements as sources that are in use.
- The categorisation of end-of-life sources as 'waste' is often incorrect and can result in import/export restrictions and may hinder transfer of the sources to an authorised site for handling.

Despite best planning, there may be a circumstance in which the return of sources to supplier or other authorised operator is not possible or practical (e.g. for regulatory reason, transport issues, closure of supplier), in which case sources may be sent to a State-recognised storage or disposal facility. If long-term storage and disposal are unavailable in the State, the responsibility for safety and security may remain with the operator. This means that the operator will continue to be responsible for maintaining security of these end-of-life sources in compliance with the requirements of their regulatory body.

## Develop Professional Competence of Staff Accountable for the Security of Sources

It is important that organisations identify positions requiring security skills, along with the necessary knowledge, skills and aptitudes to perform them effectively. Managers should ensure that individuals filling these positions are demonstrably competent through a combination of education, training and on-the-job experience. They should also manage knowledge carefully, which involves systematically identifying and organising staff knowledge and experience so that it can be retained over time. The organisation should document and evaluate professional development opportunities provided to the staff, keep records of the training, and encourage certification for security competences. Security awareness and training could be integrated with safety and/or other training, thereby minimising the time that staff are away from their job.

Professionalism can be encouraged through such avenues as:

- Certification programmes like the WINS Academy,
- Advanced degrees,
- Participation in international and regional centres of excellence,
- Membership in professional societies, and
- Participation in special training courses and workshops.

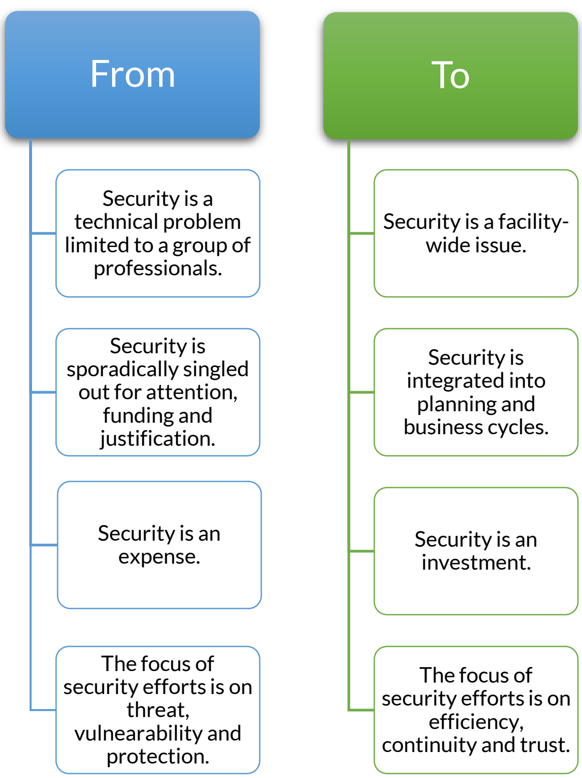
## Improve Security Culture

Security culture can be defined as:

> *The beliefs, values, understandings and behaviours that people—from the board to the general workforce—bring to security*

Experience suggests that security culture may be the single most important aspect of a security system. In an organisation with a strong security culture, staff believe that security threats are real, understand it is their responsibility to contribute to the security of the entire organisation, and adhere to security practices as a normal part of their daily work lives. If they observe an anomaly or hear something suspicious, they report it unhesitatingly to their supervisors. If they make a mistake themselves, they willingly own up to it, seek to understand how it occurred, and work actively to improve their performance. If they have ideas or suggestions for how to improve security, they share them with their managers and colleagues because they know such contributions are encouraged, respected and rewarded.

In contrast, if the security culture is weak, the workforce may resent security features and do their best to ignore or circumvent them. They may be reluctant to express concerns about aberrant behaviours and issues, materially increasing the risk for all concerned. Or they may simply forget about the need to follow basic security procedures, potentially leaving the sources vulnerable. Improving security culture requires that leadership (and subsequently the rest of the organisation) undergo a shift in perspective, as demonstrated in the following graphic.




All personnel with responsibilities for radioactive sources need to be educated about the threat and the proper procedures to follow via ongoing training sessions based on their respective accountabilities. In addition, leadership needs to make the consequences for failing to follow security procedures clear, adhere to the procedures themselves, and demonstrably enforce the consequences when the procedures are not followed correctly.

Leadership also needs to put a variety of mechanisms into place, such as a hotline or non-punitive whistleblowing policy, that clearly demonstrate they welcome communications about security concerns from their personnel. They also need to take actions that are timely, fair and appropriate to resolve such concerns.

Developing a strong security culture is an ongoing, step-by-step process. The aim should be to encourage awareness among staff of the role they play in protecting their organisation's business assets as well as the safety and security of their entire community. Consequently, this is not a one-off exercise. It needs to continue as long as an organisation uses high activity sources.

## Continually Assess and Improve Security Arrangements

It is only through the measurement of performance that an organisation can demonstrate to itself and its stakeholders that it is achieving its objectives. Performance objectives most commonly include financial, production/operational, safety and environmental performance. The measurement of **security performance**, however, can be problematic because significant challenges to the system rarely occur. This may lead management to become complacent about security and to the (potentially false) assumption that the security systems are effective. Yet a significant threat or challenge to the system could occur within minutes, leaving little or no time to address underlying managerial and technical weaknesses in the system.

For all of these reasons, measuring performance is essential for effective governance, as well as a critical aspect of building continuous improvement into an organisation's security culture. An effective performance measurement and testing programme requires the combination, integration, and management of all components that positively enhance security—or that would decrease performance outcomes if they are combined ineffectively. People, processes, technologies and environment must all be understood and managed effectively to achieve the best security outcome; failure to do so could decrease security substantially.

Poorly designed or badly implemented performance metrics can have negative consequences for the entire organisation. For example, solely collecting data on the number of security incidents provides no indication of how secure a facility actually is because incidents tend to be such rare events. Furthermore, such measures do not indicate how many attempts have been made or what the response time might be should an incident take place.

Security audits of equipment, procedures and implementation should be performed on at least an annual basis. These audits will help ensure that security is at least maintained and identify areas where improvements or modifications should be made as a result of the changing threat, other local site changes or the arrangements that an operator has with third parties. The programme of audits should also include the assessment of security during temporary operations such as cobalt-60 receipt/dispatch and installation.

In addition to internal audits and desktop and practical exercises, continuous improvement will result from cooperation with regulators and other third parties. These organisations can: assess the risks and vulnerabilities of a facility or organisation; conduct peer reviews or benchmarking against similar irradiators; and add depth and contribute to the implementation of improvements to security arrangements.

**International Support Programmes**

As an example, the Office of Radiological Security (ORS), a part of the US National Nuclear Security Administration (NNSA), works with organisations to evaluate existing security systems and provide protection upgrades, guidance and training to enhance the security of high activity radioactive sources. ORS collaborates with partner organisations worldwide on sustainable security, including implementation of regulatory development, security planning and training, transportation security, response planning and training, and the strengthening of inspection and enforcement regimes

## Harmonise Security and Safety

Both safety and security seek to protect human health, property and reputation. Furthermore, many safety features also benefit security. For example, the irradiation cell shielding also provides a layer of delay and interlock mechanisms also provide access control.

On the other hand, safety and security features have the potential to conflict with each other if a coordinated approach toward both is lacking. For example, barriers designed to prevent access by an intruder (security) could impede egress in an emergency (safety). A balance must also be struck between the desire of a radiation safety programme to have clear signage notifying persons of the presence of radioactive sources with the need to protect information related to the exact locations of radioactive sources in the facility.

These examples highlight the importance of integrating safety and security into an organisation's planning, procedures and culture. To achieve this goal, executive management needs to recognise that both are of equal importance, commit to their harmonisation, and provide adequate resources and management support to ensure that harmonisation takes place. Programmes and procedures should be conceived and developed with both safety and security in mind, in consultation with experts in both disciplines.

## Conduct Peer Reviews and Benchmarking

A peer review is a confidential, systematic process in which a group of independent, experienced practitioners in a particular field assess the quality of work of other professionals in the same field using a set of criteria and levels of performance agreed in advance with the professional community. Although the objectives and structure of peer review mechanisms vary, most involve identifying areas for improvement, sharing experience and highlighting best practices. Peer reviews are not a substitute for regulatory inspections or audits; their influence comes from the peer pressure and scrutiny that they generate, as well as from the credibility of the peer reviewers.

Peer review is an important tool for operators who are responsible for maintaining security for their radioactive sources. In recognition of this, the IAEA has extended its International Physical Protection Advisory Services (IPPAS), which was initially created for nuclear material and nuclear facilities. In Chapter V of the IPPAS guide (2014), the IAEA now provides advice to States about the security of their radioactive material, associated facilities, associated activities, and transport of radioactive material

WINS publishes guidelines for operators who recognise the value of peer review and want to conduct their own reviews. The guidance emphasises that peer reviews are designed to provide mutual support among professionals, so attitudes and tone should be collaborative, not confrontational. If either party does not understand the purpose of the peer review, then information will not flow effectively between them and the primary purpose will be lost.

### Benchmarking

Benchmarking is another effective tool for operators who want to learn best practice and evaluate the effectiveness of their security arrangements for radioactive sources. Appendix B of this guide describes different levels of effectiveness and helps operators better understand where their organisation is doing well and what needs to be done to improve weaker areas.

## Questions for Reflection

- Does your organisation take a whole-life approach toward its radioactive sources? What examples can you give to support your answer?
- Do you feel competent enough to fulfil your security responsibilities? Do you and your colleagues have access to necessary professional development opportunities regarding the security of sources?
- How would you describe your organisation's security culture? Has a security culture self-assessment ever been conducted? If so, what were the results?
- How would you describe the relationship between safety and security in your organisation? If it is not as harmonious as it should be, what can you do to improve the situation?

# CONCLUSION

Cobalt-60 sources are used in radiation processing for multiple beneficial applications. Failure to adequately secure such sources may have serious consequences for individuals, communities and the environment, as well as for the organisation's financial stability, reputation and liability. It is operators' responsibility to protect the sources in their charge and to ensure that all stakeholders—from senior management to the general staff, contractors and suppliers—understand the concepts and principles underlying the security of radioactive sources and the actions they need to take to minimise the risks.

Effectively managing radioactive source security requires that operators understand and comply with their national regulatory requirements and be aware of and implement best practices. Proper planning and execution of a layered security programme can achieve good security without an adverse impact on operations. The most important piece in maintaining excellent security, however, is security culture. All stakeholders must believe that the threat is real, understand that it is their responsibility to contribute to security on a day-to-day basis, and commit to carrying out their responsibilities to the best of their ability.

## SUGGESTIONS FOR FURTHER READING


Ashford, W. (2017, 26 July. Radiation detection devices open to cyber attack, researcher finds. *ComputerWeekly.com*. retrieved from https://www.computerweekly.com/news/450423382/Radiation-detection-devices-open-to-cyber-attack-researcher-finds

IAEA. (2010) *Radiation Safety of Gamma, Electron and X ray Irradiation Facilities*. Retrieved from https://www.iaea.org/publications/8401/radiation-safety-of-gamma-electron-and-x-ray-irradiation-facilities

IAEA. (2012) *Code of Conduct on the Safety and Security of Radioactive Sources. Retrieved from:* https://www-pub.iaea.org/MTCD/publications/PDF/Code-2004_web.pdf

IAEA. (2014). *International physical protection advisory service (IPPAS) guidelines*. Services Series 29. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/SVS-29_web.pdf

IAEA. Nuclear Security Series. Retrieved from *https://www.iaea.org/publications/search/type/nuclear-security-series*

NSS No. 7 (2017). *Nuclear Security Culture*

NSS No. 8 (2012). *Preventive and protective measures against insider threats.*

NSS No. 9. (2013). *Security in the transport of radioactive material.*

NSS No. 11. (2019). *Security of Radioactive Material in Use and Storage and of Associated Facilities.*

NSS No. 14. (2011). *Nuclear security recommendations on radioactive material and associated facilities.*

NSS No. 24-G. (2015). *Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control.*

ORS. (2018). Cybersecurity Best Practices for Users of Radioactive Sources. Retrieved from http://www.oap.go.th/images/documents/offices/baea/proap/training/ORS_Cybersecurity_Best_Practices_2018_dig.pdf

Software Engineering Institute (2013). *Unintentional insider threat and social engineering*. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

Symantec. *2019 internet security threat report*. Retrieved from https://www.symantec.com/security-center/threat-report

WINS International Best Practice Guides. Available to WINS Members at http://www.wins.org

1.4: *Nuclear security culture.*

3.4 *Managing internal threats.*

4.1 *Security by design.*

5.1 *Security of High Activity Radioactive Sources in Use and Storage*

5.5 *Security management of disused radioactive sources.*

# APPENDIX A

## Questions to assess the personal contributions to enhancing the security of radioactive sources in your organisation

Appendix A contains a series of questions that members of an organisation can use to evaluate the security of their radioactive sources. The questions also make excellent prompts for generating discussion. Such a process helps individuals at all levels of an organisation reflect critically on their personal actions and behaviour. It also helps them understand how they can contribute personally to enhancing the security of such sources within their organisation.

| Questions for Executive Management | |
|---|---|
| Do you believe the threats to your radioactive sources are credible? | ☐ Yes<br>☐ No |
| Do you understand the crucial role that leadership plays in your organisation's security culture? | ☐ Yes<br>☐ No |
| Have the board or senior management created a clear, written policy governing the security of their radioactive sources? | ☐ Yes<br>☐ No |
| Do you include the possible threat or sabotage of radioactive sources when addressing organisational risk? | ☐ Yes<br>☐ No |
| Do you know security regulatory requirements applicable to your sources? Does your security programme meet or exceed all these regulatory requirements? | ☐ Yes<br>☐ No |
| Are you familiar with the physical protection measures that are in place to keep your organisation's radioactive sources secure? | ☐ Yes<br>☐ No |
| Have you put a strong, effective human reliability programme in place to ensure the trustworthiness and reliability of your staff? Does it include pre-employment, during-employment and post-employment measures? | ☐ Yes<br>☐ No |
| Does your organisation have a well-practiced programme in place that encourages staff to share their security concerns? Do you welcome this input and take prompt action on it? | ☐ Yes<br>☐ No |
| Do you ensure that your staff regularly obtain professional development and training in security (as appropriate for their positions)? | ☐ Yes<br>☐ No |
| Does your organisation have an integrated security programme that combines conventional and radiological security? | ☐ Yes<br>☐ No |
| Do you take a whole-life approach to radioactive source management and security? Have you put effective end-of-life measures and funding in place for your disused sources? | ☐ Yes<br>☐ No |

| Questions for the Radiation Safety Officer / Security Manager | |
|---|---|
| Do you believe the threats to your radioactive sources are credible? | ☐ Yes<br>☐ No |
| Do you believe that cobalt-60 sources are self-securing due to their radioactivity? | ☐ Yes<br>☐ No |
| Do you receive periodic briefings on the threat to your sources and facility? | ☐ Yes<br>☐ No |
| Do your physical protection system include deterrence, detection, assessment, delay and response measures? | ☐ Yes<br>☐ No |
| Do you take a graded approach toward security and implement defence in depth measures? | ☐ Yes<br>☐ No |
| Do you periodically assess and measure the effectiveness of your security systems? | ☐ Yes<br>☐ No |
| Do you have a plan to continuously improve your security programme? | ☐ Yes<br>☐ No |
| Does the entire staff understand its responsibilities for security? | ☐ Yes<br>☐ No |
| Are the keys, access cards and entry codes that allow access to radioactive sources managed securely? | ☐ Yes<br>☐ No |
| Do staff receive security training when they are hired and periodically thereafter (at least once a year)? Is it effective? How do you measure this? | ☐ Yes<br>☐ No |
| Do you believe the security culture at your organisation is good? Do you conduct surveys periodically about staff attitudes toward security? | ☐ Yes<br>☐ No |
| Does executive management demonstrate strong support for security and allow you to challenge their decisions regarding security? | ☐ Yes<br>☐ No |
| Do staff understand that it is their responsibility to share any concerns they might have about security with the authorised person? Is there an established programme for this? Do staff use it willingly? | ☐ Yes<br>☐ No |
| Do you periodically conduct radiation safety and security trainings for the offsite response force? | ☐ Yes<br>☐ No |
| Do you periodically exercise your response procedures? | ☐ Yes<br>☐ No |
| Have site folders been created for all of your high activity radiation sources? Are they complete? Updated regularly? Readily available should the offsite response force require them when responding to an incident? | ☐ Yes<br>☐ No |

| Questions for Staff | |
|---|---|
| Do you believe the threats to your radioactive sources are credible? | ☐ Yes<br>☐ No |
| Do you believe you have personal responsibility for helping to maintain the security of your organisation's radioactive sources? | ☐ Yes<br>☐ No |
| Did you go through a vetting process when you were first hired? Do you believe this process helps to ensure that only trustworthy people are employed? | ☐ Yes<br>☐ No |
| Did you receive training on radioactive source security when you were first hired? Was it effective? Have you continued to receive such training periodically? | ☐ Yes<br>☐ No |
| Do you understand how to use the physical protection measures that are in place, including access measures and alarms? | ☐ Yes<br>☐ No |
| Do you willingly report any security concerns you have to the authorised person? Does management take immediate action on such reports? Are they kept confidential? | ☐ Yes<br>☐ No |
| Does management clearly demonstrate—through their actions, policies and programmes—that security is important? | ☐ Yes<br>☐ No |
| Do your managers emphasise how important it is that safety and security work together? | ☐ Yes<br>☐ No |
| Have you been trained how to protect sensitive information? Do you understand the difference between *need to know* and *need to share*? | ☐ Yes<br>☐ No |
| Do you know exactly what to do if an incident occurs? | ☐ Yes<br>☐ No |

# APPENDIX B

## Defining different levels of organisational achievement

The following chart presents five levels of security for the protection of radioactive sources, each with its own set of characteristics. By identifying where your organisation falls on this chart, you will know some steps you can take to improve the situation and move to the next level to improve the security of these materials.

| LEVEL | CHARACTERISTICS |
| --- | --- |
| 1<br>RESILIENT | Executive management demonstrate their conviction that the threat is real and that security is important by treating security as an integral part of corporate risk, by taking a risk-informed approach toward security, and by taking a whole-life approach toward the management of their radioactive sources. In addition, they have actively researched alternative technologies for their radioactive sources and converted their sources to an alternative whenever it was feasible and financially beneficial to do so.<br><br>Executive management have put a programme in place to encourage a positive security culture. This includes a human reliability programme that helps to ensure the trustworthiness and reliability of all staff and a programme for sharing concerns. It also includes conducting training in security matters at least annually.<br><br>The design of the physical protection system successfully balances deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. Security measures are well coordinated with source operation and radiation safety, and the physical protection system is regularly maintained, tested and evaluated.<br><br>Staff believe that a potential threat exists to the organisation's radioactive sources, that security is important, and that they have personal responsibility for security. They have been trained how to keep sensitive information secure, how to recognise red flag behaviours, and how to respond should an incident occur. They are also willing to share any security concerns because they know that management welcomes them and will take appropriate action while insuring confidentiality.<br><br>There is strong communication between the operator and the offsite response force, who have been trained in both radiation security and radiation safety so that they know how to respond if an incident occurs. Site/target files exist for all radioactive sources in use and storage, and they are complete and up-to-date. |

| LEVEL | CHARACTERISTICS |
|---|---|
| 2<br>PROACTIVE | Executive management generally believe that the threat is real and that security is important. They are beginning to treat security as an element of corporate risk and are usually successful at taking a risk-informed approach toward security. They also take a whole-life approach toward the management of radioactive sources. In addition, they have begun to research alternative technologies for their radioactive sources.<br><br>Executive management have put a programme in place to encourage a positive security culture. This includes a human reliability programme that helps to ensure the trustworthiness and reliability of all staff and a programme for sharing concerns. It also includes conducting refresher training in security every two to three years.<br><br>The design of the physical protection system balances deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. Security measures are fairly well coordinated with source operation and radiation safety, and the physical protection system is usually well maintained, tested and evaluated.<br><br>Most staff believe that a potential threat exists to the organisation's radioactive sources, that security is important, and that they have personal responsibility for security. They have been trained how to keep sensitive information secure, understand what red flag behaviours are, and can recognise some of them. Staff are willing to share major security concerns on an anonymous hotline, and they have a good idea about what to do if an incident occurs.<br><br>The operator and offsite response force (police) have met each other, and the officers have received basic training on radiation security and radiation safety in the event of an incident. Site/target files exist for most of the radioactive sources in use and storage, and they are usually complete and up-to-date. |

| LEVEL | CHARACTERISTICS |
|---|---|
| 3<br>COMPLIANT | Executive management generally understand that the threat is real, that security is important, and that it would be a good idea to treat security as an element of corporate risk. They have also begun to create policies and procedures that would support taking a risk-informed approach toward security. Executive management have briefly addressed what to do with disused sources that reach the end of their lives. They have also begun to research alternative technologies but have not yet come to any decisions.<br><br>Executive management generally understand the importance of a positive security culture and have put some measures in place to improve it, such as better vetting of new staff and addressing security in the overall training that new hires receive. Current staff occasionally receive refresher training in security, but not on a fixed schedule.<br><br>The physical protection system adheres to the basic regulatory requirements, but nothing more. The organisation has implemented simple provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security are all separate departments that rarely communicate with each other. The physical protection system is maintained at a minimal level. The overall effectiveness of the system is rarely tested or evaluated.<br><br>In general, staff believe that a potential threat exists to the organisation's radioactive sources and that security is important, but they do not understand their personal responsibilities for security. They have been trained how to keep sensitive information secure but have not been trained about red flag behaviours. There is a 24-hour hotline available to someone who wants to share security concerns, but it is rarely used. Staff have a basic idea about what to do if an incident occurs.<br><br>The operator and offsite response force (police) have met each other briefly, and officers have received basic training on radiation safety, but not on radiation security. Site/target files exist for most radioactive sources and are occasionally updated. |

| LEVEL | CHARACTERISTICS |
|---|---|
| 4<br>REACTIVE | Executive management do not believe their facility faces any real security threats. They assume the radiation safety officer/security director is solely responsible for security. Because they don't believe that security is an issue, they do not treat it as an element of corporate risk. Nor do they take a risk-informed approach toward security. Executive management purchase and use radioactive sources according to regulatory requirements, but they have not addressed what to do with disused sources. Nor have they considered replacing sources with alternative technologies.<br><br>Executive management vaguely understand what security culture means, but have put no measures in place to test, measure or improve it. Staff receive a handout on security issues when they are hired, but that is the extent of their training.<br><br>The physical protection system adheres to the basic regulatory requirements, but nothing more. The organisation has implemented basic provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security are all separate departments that rarely communicate with each other. The physical protection system is maintained at a minimal level. The overall effectiveness of the system is never tested or evaluated.<br><br>Staff do not believe that a potential threat exists to the organisation's radioactive sources. Nor do they understand that they have security responsibilities. They have received a brief introduction on how to protect sensitive information but do not understand or recognise red flag behaviours. There is a 24-hour hotline, but staff do not use it. Staff have only a vague idea about what to do if an incident occurs or who would be in charge.<br><br>The operator and offsite response force (police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Site/target files exist for major radioactive sources, but they are rarely updated. |

| LEVEL | CHARACTERISTICS |
| --- | --- |
| 5<br>VULNERABLE | Executive management do not believe their facility faces any security threats. They assume that the radiation safety officer/security director is solely responsible for security. Radioactive sources are generally purchased according to regulatory requirements, but no provision has been made for disused sources. Management have no intention to replace sources with alternative technologies.<br>Executive management do not consider security culture to be a risk. The only emphasis in staff training is on safety issues.<br>The physical protection system generally adheres to the basic regulatory requirements, but sometimes falls short. The organisation has implemented a few elements of deterrence, detection, delay and response, but has not taken a systematic approach for doing so. Source operation, radiation safety and radiation security do not communicate with each other. Maintenance of the physical protection system is minimal.<br>Staff do not believe that a potential threat exists to the organisation's radioactive sources. Nor do they understand that they have security responsibilities. Furthermore, they have not received any training on how to protect sensitive information, there is no provision for sharing concerns, and they have no idea what to do if an incident occurs or who would be in charge.<br>The operator and offsite response force (police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Furthermore, there are no site/target folders. |