World Institute for Nuclear Security

A WINS International Best Practice Guide

GROUP 5: Security of Radioactive Sources

5.5 Security Management of Disused Radioactive Sources

Version 2.0

SECURITY MANAGEMENT OF DISUSED RADIOACTIVE SOURCES

A WINS International Best Practice Guide

Why You Should Read This Guide

Thousands of radioactive sources worldwide come to the end of their working life each year. Most organisations anticipate this and arrange in advance to exchange an old source for a new one or to return the disused source to the original supplier. However, some users fail to plan for end-of-life management and for the costs associated with transportation and disposal. As a result, they may decide to store them for an extended period, often under substandard conditions. This may result in a gradual loss of awareness and subsequently lead to deficiencies in the control of the disused sources. This creates unnecessary safety and security risks.

Disused sources that are not properly managed are more likely to become misplaced, lost or stolen. The majority of radiation accidents involving death or injury have been caused by disused sources[1]. It is therefore imperative that disused sources are handled with the same level of attentiveness as sources that are still in use. Users who fail to properly plan for the end-of-life management of their sources could not only expose their staff and community to unnecessary safety and security risks, but themselves and their organisation to significant liability.

If your organisation uses radioactive sources, you should be concerned with safety and security of radioactive sources throughout their lifecycle. Executive and senior management, radiation safety officers, security managers and operational staff all have a role in development of an effective and comprehensive safety and security culture that will manage risk at a site that uses radioactive sources. In particular, end-of-life management of disused sources may pose a challenge to an organisation. A disused source is typically viewed as less valuable, and attention in an organisation may wane, especially if it is stored over an extended period of time. This may lead to less attention being given to source security. However, the secure management of disused radioactive sources should be an important concern, as a security event involving disused radioactive sources would create significant consequences for your organisation. You will want to make sure that your senior management is aware of the risk and provides adequate resources for the secure management of disused sources. Your first concern will be to understand and comply with your national regulatory requirements in order to avoid enforcement action from regulators for exposing workplace personnel, the public and the environment to avoidable harm. If national regulations have not been established, responsible professionals will still wish to take sensible steps to secure disused sources. Even if no legal sanctions are in place, your organisation's reputation will be damaged if it is later shown to be responsible for a harmful event and your customers might distance themselves from your organisation.

A security system to protect disused sources is essentially the same as a security system for sources in operational use. However, some of the challenges differ, especially with respect to the mind-set of those with responsibilities for end-of-life management of radioactive sources. Sources that are not in daily use are not seen as an asset that needs protecting, but they still present risks and their security must be managed accordingly.

[1] A number of detailed reports of accidents involving disused sources can be found in the IAEA Publications on Accident Response: http://www-pub.iaea.org/books/IAEABooks/Publications_on_Accident_Response

This WINS Best Practice Guide (BPG) provides an introduction to important issues specific to end-of-life management of disused sources, in particular how to maintain an appropriate level of security until their final disposal. It discusses current arrangements for exchanging and/or disposing of disused sources and several approaches to end-of-life management. It also discusses some possible challenges, such as how to make financial provision for end-of-life disposal. This BPG should be read in conjunction with the other WINS publications relevant to radioactive sources.

About the Appendices

Appendices A and B provide a series of questionnaires and indicators of levels of organisational competencies relating to the end-of-life management of disused sources. Appendix A provides a set of questions that can be asked at all levels of an organisation to help determine how effective the current arrangements are for the secure management of disused sources during storage, transport and disposal. Appendix B defines five different levels of organisational achievement for security. 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 actual experiences of security practitioners and managers of disused sources. This revision draws on discussions and outcomes from the International Best Practice Workshop on the Security of Disused Radioactive Sources organised by WINS and ISSPA in Vienna in October 2019.

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 plan to update the information in this guide periodically to reflect best practices and new ideas. Therefore, we ask that you read it carefully and let us know how it can be improved. Please email your suggestions to info@wins.org. If you have ideas for additional WINS Best Practice Guides, we would like to hear about them. WINS is committed to working with nuclear security professionals; our vision is to share best practices to achieve operational excellence.

Dr Roger Howsley
Executive Director

April 2020

WINS Contact Information

World Institute for Nuclear Security
Landstrasser Hauptstrasse 1/18
A-1030 Vienna, Austria

Email: info@wins.org
Phone: +43 1 710 6519

www.wins.org

Version 2.0
ISBN: 978-3-903191-71-6
WINS (20)20

CONTENTS

UNDERSTANDING THE RISK 4

THE RADIOACTIVE SOURCE LIFECYCLE 7

THE INTERNATIONAL FRAMEWORK FOR THE SECURITY OF DISUSED SOURCES 9

THE NEED FOR A NATIONAL STRATEGY AND EFFECTIVE REGULATIONS 10

PLANNING TO MANAGE THE SECURITY OF DISUSED SOURCES: THE EARLIEST STAGES 12

A PROCESS FOR DESIGNING AND IMPLEMENTING SECURITY MEASURES FOR DISUSED SOURCES 14

Understand Your Role and Responsibilities for Disused Sources 15
Develop a Robust Security Culture 15
Define and Address the Threat Environment 15
Understand the Targets for Malicious Acts and Their Possible Vulnerabilities 16
Apply a Graded Approach, Provide Defence in Depth and Ensure Balanced Protection 16
Design the Security System 17
Draft a Security Plan 18
Protect Sensitive Information 18
Develop an Effective and Coordinated Response Strategy 18
Implement and Sustain Your Security System 18

OPTIONS PRIOR TO SEEKING DISPOSAL 19

Reuse 19
Recycling 19
Conditioning: Preparing Sources for Interim Storage 19

DISPOSAL OF DISUSED SOURCES 20

SUGGESTIONS FOR FURTHER READING 22

APPENDIX A 23

APPENDIX B 27

UNDERSTANDING THE RISK

Human beings and the environment could be harmed significantly if a high activity radioactive source—whether still in use or disused—is lost from adequate control and is accidentally found by someone who is unaware of its dangers or is intentionally stolen by someone with malicious intent. It could create significant public concern, and in case of radioactive contamination, the associated clean-up and liability costs could be substantial. Furthermore, the public relations issues could negatively affect confidence in the industries using radioactive sources. Properly managing radioactive sources, even when they are disused, is vital.

Although it has never been used, one method by which terrorists or criminals could use radioactive material for a malicious purpose is in a radiological dispersal device (RDD), which is created when conventional explosives such as dynamite are used to spread radioactive material. RDDs, or dirty bombs, are not considered to be a weapon of mass destruction because they would not have the same magnitude of effects as a nuclear device. Immediate casualties from an RDD would be the result of the bomb itself, not of radiation, and there would be no nuclear detonation.

However, people in the area could be exposed to radiation either externally or internally (by inhaling or ingesting radioactive particles). The surroundings could also be radioactively contaminated, potentially denying their use for a long period of time. In a city (for example), the level of disruption this would cause could be extreme. Remember – this could be achieved with a disused source.

Experience shows that the public and the media react strongly to any events involving radioactivity, even when the level of hazard is low. It is important, therefore, to appreciate that most disused sources (although no longer suitable for their intended purpose) could be just as useful to people with malicious intent as a new source, and that they should therefore be managed with an appropriate level of security.

What we mean by disused radioactive sources

When radioactive sources are no longer effective for their intended purpose, they become disused. This can happen for a variety of reasons. The major one is that the potency of radiological sources declines over time and their lifecycle eventually ends.

Some sources may still be potent, but their housing becomes damaged. Others become obsolete as new technologies are developed. Sometimes the licensee no longer performs the same activity or ceases operations altogether.

It is important to appreciate that because a source has become disused, it is not necessarily no longer hazardous. In reality, the reverse is true: Most disused sources are still of radiological concern even if they are no longer fit for their intended purpose.

To date, only a few incidents have occurred in which radioactive materials have been used or planned to be used to harm an individual. However, authorities around the world continue be concerned that terrorist groups, criminals or other adversaries will attempt or are attempting to do so, and the threat that an event could occur in the future remains high.

However, in hundreds of cases around the world, radiological sources have been inadvertently acquired by people unaware of their danger—particularly scrap metal dealers—and they and their communities suffered severe consequences as a result. The following four examples indicate how much harm can be caused by accident. It is evident that with the addition of malicious intent, a great deal more harm might ensue.

Example 1: Mexico

In December 2013, a truck driver in Mexico was transporting a disused teletherapy device from a hospital in Tijuana (on the US border) 2,900 kilometres south to a disposal site near Mexico City. Shortly before arriving at his destination, he pulled into a truck stop and fell asleep. He was awakened by two armed men who stole the truck. Authorities quickly found the truck and the device in the vicinity of where they had been stolen. The source had been removed from the device, but its protective cover was not damaged. Consequently, no harm to human life or the environment likely occurred. However, the potential for disaster was great; the strength of the cobalt-60 was 3,000 curies (111 TBq), making it a Category 1 source. Category 1 sources are the most dangerous of the IAEA's five levels of radioactivity and can cause permanent injury to someone who comes into contact with them within minutes; death can occur within minutes to one hour.

Example 2: India

In 2010, the University of Delhi in India began a campus-wide effort to remove and dispose of unwanted objects. One of these items was a disused instrument that hadn't been used in 25 years. The university staff did not know that it contained cobalt-60. The object was auctioned to a scrap metal dealer in Mayapuri. The buyer cut off some of the metal and gave it to another scrap metal dealer, who put it in his wallet. In less than a month, the shop owner was hospitalised with radiation sickness, as was the other scrap metal dealer. In the end, eight people were hospitalised and one person died. Authorities eventually recovered eight sources at the original shop, two sources at a nearby shop, and one from the dealer's wallet. They also had to remove contaminated soil.

Example 3: Thailand

In February 2000, the radioactive source of a disused teletherapy unit was purchased illegally, without registration, in Samut Prakarn, Thailand. The unit was then stored in an unguarded parking lot without warning signs. Scrap metal dealers soon discovered it and took it to their junkyard, where they completely removed the cobalt-60 source from the lead shielding. They became ill soon after, but 18 days passed before the radioactive nature of the metal and the resulting contamination were discovered. The incident ultimately led 10 people to be hospitalised for acute radiation exposure, three of whom died.

Example 4: Brazil

The most serious example of what can happen when highly active sources are abandoned occurred in 1985 in Goiânia, Brazil.

A private radiotherapy institute moved to new premises, leaving in place a caesium-137 teletherapy unit without notifying the licensing authority as required under the terms of the institute's licence. The former premises were subsequently partly demolished. As a result, the caesium-137 teletherapy unit became totally insecure. Two people entered the premises and, not knowing what the unit was but thinking it might have some scrap value, they removed the source assembly from the radiation head of the machine, took it home and tried to dismantle it. They eventually got to the source capsule, which contained 1,200 Ci (44.4 TBq) of caesium-137, and removed it.

The men began to feel ill the same day they began dismantling the unit, but they continued with their work. Two days later, they sold pieces of the unit to another scrap metal dealer, who in turn sold the pieces to others in the community. People were especially intrigued by a blue glow that the material was giving off, and some spread it across their skin. (This rarely occurs but was due to moisture from perspiration).

In the coming days, alert hospital staff recognised symptoms of acute radiation syndrome (ARS) in a number of victims. The ensuing panic eventually caused more than 112,000 people—10% of the

population—to request radiation surveys to determine whether they had been exposed. At a makeshift facility in the city's Olympic Stadium, 250 people were found to be contaminated. Twenty-eight had sustained radiation-induced skin injuries (burns), and 50 had ingested caesium.

Tragically, two men, one woman and one child eventually died from acute radiation syndrome. One of the two scrap metal dealers who originally dismantled the unit had to have several fingers amputated, and the other one had to have an arm amputated. In addition to the human toll, contamination was tracked over roughly 40 city blocks. Of the 85 homes found to be significantly contaminated, 41 had to be evacuated and seven had to be demolished. Within a short period of time, houses located 160 kilometres away from the site were found to be contaminated due to the routine travel of people in the community. Clean-up efforts eventually generated 3,500 cubic metres of radioactive waste at a cost of $20 million.

Furthermore, the impact of the incident led beyond physical effects and damage to profound psychological trauma, including fear and depression, for a large fraction of the city's inhabitants. Frightened by the spectre of radioactive contamination, neighbouring provinces isolated Goiânia and boycotted its products. The price of their manufactured goods dropped 40%, and tourism, a primary industry, collapsed. Total economic losses were estimated at hundreds of millions of dollars and reportedly took ten years to recover.

The IAEA called Goiânia one of the world's worst radiological incidents. Today it can be considered a textbook case of what can happen when disused high-activity radioactive material goes out of regulatory control, is left unsecured, and is eventually found by people who have no knowledge of its dangers. Even greater consequences could ensue if such material is stolen by people with malicious intent who plan to maximise the harmful impacts.

In today's world of social media and 24/7 news coverage, similar stories would travel around the world almost instantaneously, and the social, political and media consequences for all concerned would be significant, even in cases where the radiological consequences may not be so extensive. Adverse publicity of this kind can seriously damage a business and could realistically cause it to shut down.

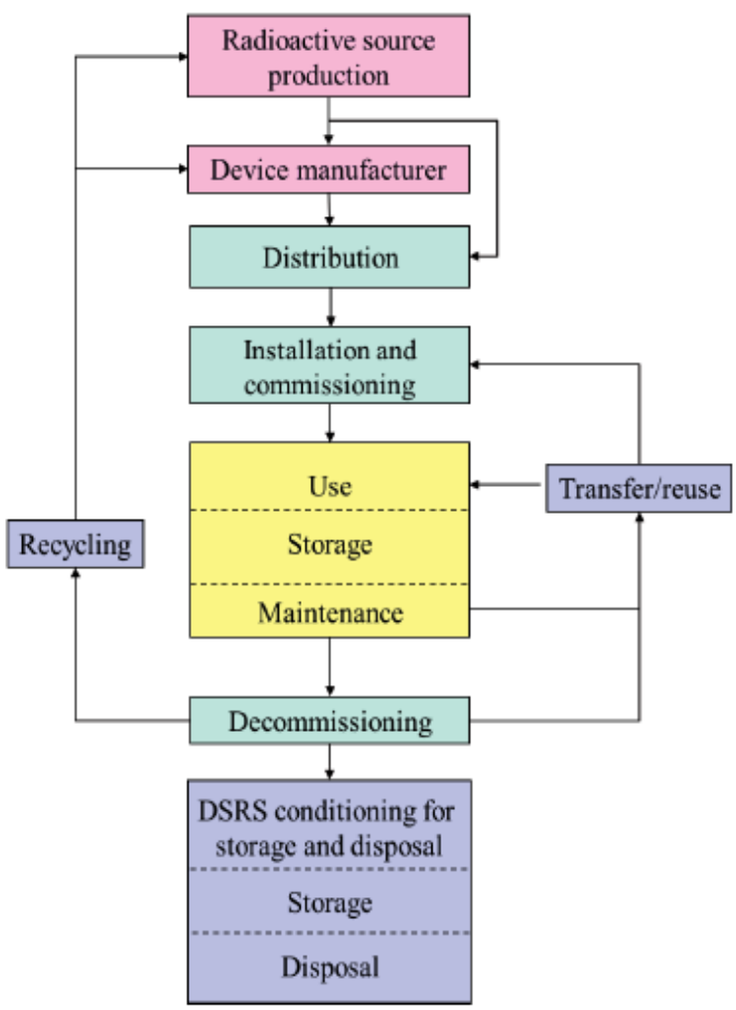
THE RADIOACTIVE SOURCE LIFECYCLE

Effective management of radioactive sources must include a safety and security strategy that encompasses the source lifecycle, including end-of-life management of sources. This would include the following aspects of the source lifecycle: the original purchase; source licensing; the active use or application of the source; its transition into disuse; provisions for decommissioning, exchanging, reusing and recycling the disused source; decommissioning of the source; interim onsite or offsite storage; source conditioning for transportation; transportation offsite; and ideally final disposal in a permanent State-licensed and approved repository.

A lifecycle approach requires the necessary personnel and financial resources, as well as carefully planned and implemented procedures, policies and records. It also requires implementation of a system for handling sensitive information and for protecting it from unauthorised disclosure.

If this sensitive information is stored digitally on a corporate information technology infrastructure, it is important to protect the infrastructure from cyberattacks that could lead to vulnerability in the security of radioactive sources.

As shown in the following figure, the lifecycle of a source can follow many routes before it is conditioned for final disposal. (In the diagram below, DSRS refers to disused sealed radioactive sources). It is important to understand that the prerequisite to effective management of the source lifecycle is a regulatory and legal infrastructure in conjunction with a robust security strategy.



Generic lifecycle of a sealed radioactive source (IAEA NW-T-1.3)

Sources begin their lifecycle when the radioactive material itself is created in a nuclear reactor. The material is then encapsulated by a source manufacturer and becomes a sealed radioactive source. This radioactive source could then go to an equipment manufacturer, where it is inserted into a variety of devices depending on its intended use. Users buy the device from the manufacturer or from a distributor who is licensed by the manufacturer to sell the product.

Some sources are supplied without being part of devices. For example, those used for iridium-192 industrial gamma radiography may be shipped from the source manufacturer/supplier in a shielded container with a number of other sources to be loaded in gamma projectors at their destination. Similarly, cobalt-60 sources used in industrial irradiators may be transported in special licensed transport packages to the end user for installation as new or replacement sources.

For one reason or another, a source will eventually become disused. When it does, it needs to be appropriately decommissioned so it can be returned to the supplier, conditioned and stored, or sent for disposal at a proper disposal facility.

Why Do Sources Become Disused?

There are several factors that may lead to radioactive sources becoming disused. These include:

- The activity decays below the minimum required for the specified purpose
- The source becomes damaged or leaks
- The device containing the source becomes obsolete
- An alternative technology may emerge, making the one using the source redundant
- A company may change its priorities, for example, ending a programme of work involving sources

When a previously useful source falls into disuse—for whatever reason—there is a danger that its perceived importance is significantly reduced due to its lack of value: It no longer generates income and organisations may assume spending money on the end of its life is not worthwhile. This is absolutely not the case: The business risks are reduced by investment in prompt disposal, or where this is not possible, then investment in appropriate levels of security for disused sources.

The next section briefly reviews the international recommendations and guidance provided to States to develop a global approach to effective security management of radioactive sources. It provides some background on where the requirements have come from that your national regulator applies to licensed users about the security of disused sources. The rest of this document is intended to help users understand how to plan and manage the security of disused sources. The document does not provide detailed guidance on how to design and implement a comprehensive security programme. The reader is encouraged to read other WINS materials relevant to radioactive sources, including BPGs, Special Reports and workshop materials; to exchange lessons learned and experiences with other disused sources practitioners; and if necessary, to seek the assistance of security experts.

THE INTERNATIONAL FRAMEWORK FOR THE SECURITY OF DISUSED SOURCES

The IAEA has developed a non-binding international and inter-governmental *Code of Conduct for the Safety and Security of Radioactive Sources*[2], as well as recommendations and guidance on the security of radioactive sources. These instruments have been primarily designed to assist Member States in developing a national policy and strategy for managing source security throughout the source lifecycle.

The *Code of Conduct* provides high level guidance for the development, harmonisation and implementation of a national strategy for the safety and security of radioactive sources. This includes policies, laws and a system of regulatory control for the safety and security of radioactive sources, all important and necessary measures to regain control over lost, missing and orphan sources.

The primary objectives of the *Code of Conduct* are to:

i. *Achieve and maintain a high level of safety and security of radioactive sources;*
ii. *Prevent unauthorised access or damage to, and loss, theft or unauthorised transfer of, radioactive sources, so as to reduce the likelihood of accidental harmful exposure to such sources or the malicious use of such sources to cause harm to individuals, society or the environment; and*
iii. *Mitigate or minimise the radiological consequences of any accident or malicious act involving a radioactive source.*

The *Code of Conduct* states: "These objectives should be achieved through the establishment of an adequate system of regulatory control of radioactive sources, applicable from the stage of initial production to their final disposal, and a system for the restoration of such control if it has been lost." This opens the way for development of a national strategy, which is discussed further in this Best Practice Guide.

Two documents supplement the *Code of Conduct* and are beneficial to the development of a national strategy and to enhance the overall security framework during the radioactive source lifecycle.

The supplementary *Guidance on the Import and Export of Radioactive Sources* "aims to provide guidance for an adequate transfer of responsibility when a source is being transferred from one State to another." While the Guidance applies to Category 1 and Category 2 sources, the principles in the Guidance may apply to other sources as well. The document is helpful to suppliers and those who will purchase and/or use the source. It enhances sensitivities around lifecycle safety and security of the sources involved in a commercial transaction. It also facilitates a review by exporting States to determine whether the importing State has a suitable regulatory system in place to manage sources that come under the jurisdiction of the importing State.

The supplementary *Guidance on the Management of Disused Radioactive Sources* received significant international support from regulators and industry that led to its development, preparation and release as a published document in 2018. National and international regulators, suppliers, users and industry associations were actively involved in preparation of the Guidance document.

Within the context of the overall lifecycle management of radioactive sources, the objective of this document is to encourage States to improve the safety and security of disused sources in line with the provisions of the Code. The intent is to identify actions to be taken, starting with the decision to acquire a radioactive source and continuing through disposal, to ensure that disused sources are safely and securely managed.

[2] http://www-pub.iaea.org/MTCD/publications/PDF/Code-2004_web.pdf

> The document is also intended to advise States on the available management options for disused sources. These options, described further in this BPG, include reuse or recycling, long-term storage and disposal, and return to a supplier. Short-term storage and transport, which are addressed in the Supplementary Guidance, are not considered as options in themselves but are often necessary interim steps in the implementation of options. The Supplementary Guidance also considers return to sender an option but is not intended "to place the sole responsibility for the management of disused sources on the Supplier State nor to ascribe obligations on other States to take back sources they may have previously supplied."

As reported on the IAEA's NUCLEUS information resource portal, it is noteworthy that as of 22 January 2020, 140 States had made a commitment to implement the *Code of Conduct* and only 35 of them had expressed support for the *Guidance on Management of Disused Sources*. While it is encouraging to see progress has been made, it is apparent that considerable effort by Member States is still required to adopt international recommendations fully and ensure comprehensive safety and security of radioactive sources throughout their lifecycle.

THE NEED FOR A NATIONAL STRATEGY AND EFFECTIVE REGULATIONS

Maintaining effective control over the entire lifecycle of radioactive sources requires a properly functioning legal infrastructure. Many countries already have robust laws and regulations for governing nuclear safety and radiation protection. However, this is not always the case when it comes to the security of radioactive sources. Some Member States do not yet have a national strategy, nor have they established comprehensive regulatory requirements for the security of radioactive sources, especially when they become disused.

As an example, at the WINS Workshop on the Security of Disused Radioactive Sources in October 2019, 35% of participants reported that their country does not yet have a well-established national strategy for managing disused sources, and 25% challenged the ability of their regulatory requirements to effectively support the management of disused sources. Only 45% of them thought their country had effective arrangements for returning sources to suppliers and less than 40% thought their country had a clear plan for long term-storage and disposal of disused sources. These results, as well as some other workshop outcomes, indicate that there is still substantial work to do in certain areas to establish an effective national policy and strategy to manage disused sources.

States can draw on the international framework to establish their own national strategy to maintain regulatory oversight of the security of radioactive sources during the source lifecycle. The regulatory authority within each State is responsible for establishing and enforcing the codes and regulations that users and other stakeholders must follow to ensure the safety and security of the materials for which they are responsible. International organisations also provide some guidance for operators in regard to effective implementation of the requirements.

When developing a national strategy for managing disused radioactive sources, States should consider the following questions:

- Is the role of the manufacturer, supplier and user clearly defined?
- Is end of life clearly and effectively addressed in the regulatory and licensing process?
- Have reuse/recycling options been adequately explored and developed?
- What provisions are in place on the export/import documentation that would facilitate return of sources to the original supplier?
- Are interim storage arrangements effective and secure?
- Are licensed resources available to condition sources for packaging, transport and disposal?
- Are suitable, licensed transport packages available to facilitate source transfer to a suitable facility or repository?
- Has a clear, well-defined pathway for long-term storage and disposal been established? Are suitable repositories available?
- Is a process in place to record and share lessons learned or best practices for disused source management between organisations?
- Are cybersecurity matters considered for the secure management of disused radioactive sources?
- Is there a take back agreement with the supplier or a financial instrument in place to cover the cost of removal or disposal?

What Should Happen to a Disused Source?

Storing disused sources on the premises of end users with no specific purpose is not a good practice. Once the source becomes disused, a distributor or manufacturer should ideally supply a new one and take the old one back. Suppliers generally have the capacity to safely and securely manage the radioactive sources they provide. They are also better able to determine whether disused sources can be reused, recycled or assigned for final disposal. However, these arrangements have not always been in place, and even today they may not always be practicable when international transactions are involved.

In some cases, the disused source may be placed in long-term storage or at a State-recognised storage or disposal facility, rather than returned to the manufacturer or supplier. When transferring disused sources to a long-term storage or disposal facility that is recognised by the State or the regulatory body, it is important to ensure that the legal responsibility for the safety and security of those sources is transferred from the user to the operators of the disposal facility. Unfortunately, many States do not have this option and the responsibility remains with the user, perhaps for decades. The user is then faced with doing the best they can, depending on their local circumstances and ensuring they comply with the regulatory requirements still applicable to them.

PLANNING TO MANAGE THE SECURITY OF DISUSED SOURCES: THE EARLIEST STAGES

Planning for the end of life ideally needs to start even before the sources are ordered. It is recognised that this is not feasible for the many thousands of sources that were supplied years ago and are soon to fall into disuse, nor for those which are already in storage pending disposal. But it is beneficial to outline some of the thinking that can be applied before acquiring new sources in the future, in anticipation of the need to manage them effectively when they become disused years or decades in the future.

Some of the ideas given below need to be established by regulators, usually in cooperation with national and international industrial stakeholders, including source designers and manufacturers, device suppliers and distributors, users and radioactive waste management organisations. However, some would likely be of use at the user level to facilitate planning for the end of life, depending on national circumstances and especially national financial legal systems.

Experience shows there are a number of barriers to the prompt disposal of disused sources. One of the biggest barriers is the cost. Source disposal can be expensive without proper planning and difficult or even impossible to afford if a company is going through a difficult business period. However, if a user identifies the range of ways in which the end-of-life disposal of a source can be funded and otherwise planned for in advance of even ordering them, it is likely to significantly ease the difficulties. The next section considers disposal funding options.

Take Back or Source Replacement Agreements

When the source is ordered, the supplier may agree that at the end of its life, the source will be returned to the supplier and any costs of take back are included in the purchase price or addressed in terms and conditions in the purchase contract. In the case the source is expected to be returned to the supplier and replaced with a new one, the cost of removal and disposal of the final source may only be included in the last purchase contract. Take back and source replacement agreements are considered the preferred mechanisms.

Leasing Arrangements

Some contracts between source suppliers and users specify that ownership of the source remains with the supplier. At the end of life, the source is returned to the supplier. The cost of removal is included in the leasing price. Some leasing agreements may exclude the costs of transport of the sources at the end of their useful life. Any such exclusions should be identified before an order is placed so financial provision can be made to pay these end-of-life costs.

Decay Storage

Ideally this should only be used where at the end of proposed life the source will have decayed to below IAEA Basic Safety Standards (BSS) exemption levels. This may mean it can be lawfully disposed of with non-radioactive waste—but check with your regulatory body before doing so. However, it should be recognised that this is a limited option that will only be relevant in the case of radionuclides with a short half-life.

Other types of approach involve planning to provide financial resources to cover end-of-life costs for each relevant source. These are outlined below.

Public Sector or Government Underwriting

In some countries, all sources are owned by the government and they are therefore responsible for the costs of disposal of disused sources, rather than the "front line" user. Alternatively, a government department may commit to covering the costs of the sources used within their jurisdiction, such as the health system.

Accounting Approaches

These approaches will vary from State to State according to the financial legal code. The intention is to illustrate ideas that may be adapted for local implementation.

- Making provision in accounts

  An organisation may set aside funds in its accounts every year, in anticipation of having to spend them years or decades in the future on the costs of disposal of their disused sources. This is an accounting measure, not a cash fund. The disadvantage of this arrangement is that it may be difficult to ensure that the funds are not affected if the organisation goes out of business.

- Charged funds

  Under this system, users can set aside cash in a separate account to fund the estimated disused source management costs over which a third party holds a charge. This could be the regulatory body or a radioactive waste management company acting on behalf of the regulator. The charged funds may be able to be set aside or drawn from the holders' other assets and liabilities and are available to meet the costs of disused source management in the event of the user going out of business.

- Third party guarantees

  Users can obtain a guarantee (for example a bond or a letter of credit) in respect of their disused source management obligations from a third party (a "bondsperson"). Usually, such guarantees are provided by banks or other financial institutions. In the event of the holder being unable to meet his obligations, the third-party guarantee can be "called in". To the lay person, this is similar to an insurance arrangement, but it involves only two parties and not a whole market of insurees.

The costs of any of these arrangements must be tracked in subsequent years' budgets and properly managed to cover inflation and unforeseen costs.

A PROCESS FOR DESIGNING AND IMPLEMENTING SECURITY MEASURES FOR DISUSED SOURCES

This section presents what you need to know and understand for effectively protecting disused sources and adequately managing the risks. In particular, it will provide you with a detailed 10-step process (derived from BPG 5.1) to follow for identifying and implementing specific security measures. However, specialist assistance may be required for some of the steps in this process. (It is important that you read this section in conjunction with other WINS BPGs relevant to radioactive sources, such as BPGs 5.1 to 5.4, in so far as they apply to your own circumstances.)

1. Understand roles and responsibilities.
2. Develop a strong security culture.
3. Identify and address the threat environment.
4. Understand the targets for malicious acts and their vulnerabilities.
5. Apply a graded approach, provide defence in depth and ensure balanced protection.
6. Design the security system.
7. Draft a security plan.
8. Protect sensitive information.
9. Develop an effective, coordinated response strategy.
10. Implement and sustain your security system.

These steps will provide you with useful guidance to understanding the approach that should be taken to establish your own security system and to ensure that the desired security outcomes are likely to be achieved. These steps must, of course, be considered with relevant political, national and cultural factors specific to your circumstances.

Although most of these steps are the responsibility of the user, many of them include items that a State regulator is likely to focus on when issuing regulatory requirements, granting operating or possession licences, and assessing your level of compliance. However, even if you are not yet subject to detailed regulation on these matters, it makes good business sense to follow this list to secure your own sources. This is the best way to manage the business risks.

Understand Your Role and Responsibilities for Disused Sources

It is important that your organisation recognises that its responsibilities extend over the whole lifecycle of the sources they use, including once they become disused. This means that all those with responsibilities need to be properly informed, whatever their level in the organisation. This can be accomplished by applying the principles imbedded in a continuous improvement programme, using periodic training and review sessions, as appropriate, to raise awareness. Recognising that the timescale of these responsibilities is likely to be extended and very different from the sources that are in operational use, it is important that senior managers, supervisors, radiation safety officers, security managers and operating personnel are all aware of the nature of the challenges of keeping disused sources securely pending final disposal.

Users should always bear in mind that the storage of disused sources at their premises should be considered an interim measure only and they should be retained for as short a time as possible. They should remember that the sooner a source that has no real function is moved to a location equipped to reuse, recycle or permanently dispose of the source, the lower the risk is for the organisation.

Appendix A to this document will be helpful in assessing the level of awareness and commitment in your company to source security oversight as well as for planning and developing a continuous improvement programme to effectively manage source security. This is a key step in achieving the next item in the list: developing a robust security culture.

Develop a Robust Security Culture

Protecting the physical assets of your organisation is simply common sense. You prevent loss and theft of valuable assets whether they are equipment used to provide the service that your business is based on (such as sources) or the policies, procedures and records that mean you can manage the income and cost associated with operating your business. Executive and senior managers in the organisation should show leadership in recognising that the corporate responsibilities include disused sources. It would be appropriate, for example, for senior staff to challenge junior colleagues about their appreciation that security of disused sources is as important as that of those that are in regular operational use.

It would also be appropriate for management of radioactive sources to be a standing agenda item for executive committee meetings as well as a topic for annual general meetings and annual reports. Inclusion of disused sources in these oversight matters will keep the issue foremost in the minds of all those involved. Finally, staff can be appraised as part of their performance review on their awareness of security of disused sources. A key point here is: This is not a “one off” exercise. Periodically, the security culture of your organisation needs to be reassessed and refreshed as appropriate—this is a key tenant of any continuous improvement programme. If this does not happen, disused sources may particularly be vulnerable to degradation of their security.

Define and Address the Threat Environment

Understanding the motivations and modus operandi of both external and insider adversaries is crucial when it comes to creating a security strategy, programme and plan for mitigating the threat to disused radioactive sources. You need to clearly understand who potential adversaries are and what they are capable of doing. How easy would it be for them to access sources at your premises? What tools would they need? How would they go about doing it? How long would it take? How might they remove the source with minimum exposure to themselves? Could they simply steal the device containing the source?

It is usually the responsibility of national authorities to analyse the potential threats to nuclear and other radioactive materials. These analyses take into account such factors as local terrorist and criminal activity, recent security incidents, history of nuclear and radiological smuggling, and level of criminality and corruption. If your national authorities have not performed a national threat assessment or communicated to you the threats applicable to your sources, you should perform your own basic threat assessment to identify a baseline of potential characteristics and attributes for adversaries that could target your activities. This could be carried out with the assistance of security consultants and/or in coordination with local law enforcement agencies.

Understand the Targets for Malicious Acts and Their Possible Vulnerabilities

Security issues pertaining to disused sources do not differ much from sources still in operational use. Even if these sources are no longer radioactive enough to be used for their intended purpose, they can still be harmful and attractive to an adversary. Therefore, disused sources need to be included in a programme of security measures, taking into account regulatory and corporate risk management requirements. Security arrangements need to be assessed periodically and any potential vulnerabilities mitigated.

Lack of attention to disused sources, and therefore of assigned resources to their proper management, is a common situation of increased safety and security risk. It is good practice to add disused sources to the risk register of your organisation and include them as part of the various management reviews and other periodic audits.

Apply a Graded Approach, Provide Defence in Depth and Ensure Balanced Protection

Graded Approach

As you would do for sources in operational use, apply the greatest degree of security to the disused sources that would have the highest consequences if they were stolen by a malicious adversary. This means that if any disused sources have decayed to levels that are not likely to be hazardous, then fewer security measures are required to protect them. This means that costs can be focused on the greatest security need and less money may need to be spent where the risks are lower. However, it should be remembered that even sources categorised as “exempt” can cause disruption, create liabilities and damage reputations.

Defence in Depth

Defence in depth consists of installing multiple and diverse layers of protection around the asset (target) to be protected. 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 location—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.

Balanced Protection

The design and performance of the security functions of deterrence, detection, delay, response and security management should be balanced to provide adequate protection against all threats along all possible adversary pathways. The outcome of a balanced protection system for disused sources will be that they do not have any vulnerabilities which are left unidentified and unaddressed. (For example, do not be fooled by suspended ceilings: How secure is the void above it?) This is best achieved by consolidating all the points above into a single security system whose scope includes both disused sources and sources in operational use.

Design the Security System

Ideally, a security system should be designed and implemented in advance of the receipt of radioactive sources, and therefore well in advance of radioactive sources becoming disused. In reality though, many users will have a long-existing inventory of sources which may well include a number of disused sources. This means that part of the design process should be to consider whether a phased approach would meet the requirements of the regulatory body and otherwise assist in implementation. This would enable a time limit to be set to achieve a suitable level of security, while optimising the rate of expenditure.

The overall objectives of a security system are to deter adversaries from trying to steal the source or disused source and minimise the likelihood an adversary will successfully steal the material. This requires a combination of technical, human and administrative measures with which to detect and assess any attempts to access the source location and to delay adversaries until an adequate response force (e.g. the police) can arrive and interrupt, or neutralise, them. These security functions are discussed in more detail in BPG 5.1 but are summarised below:

Deterrence occurs when an adversary is dissuaded from undertaking a malicious act because they recognise that it would be too difficult to mount, success would be too uncertain, and the consequence would be too unpleasant. Examples of deterrence measures include good lighting, fences, CCTV cameras, visible guards and patrol dogs.

Detection is the discovery of an attempted or actual intrusion undertaken to remove material or sabotage a radioactive source. Examples of detection measures include visual observation, video surveillance, electronic sensors, material control and accountancy records, seals and other tamper-indicating devices, and process monitoring systems. Remember: Someone needs to be assessing these means of detection to decide whether they are real and require a response or are false alarms.

Delay measures, such as fences, locks and window bars help to increase the time it takes adversaries to gain unauthorised access and remove radioactive materials. Robust walls required for safety purposes may function as effective security barriers as well.

Response refers to the actions undertaken by onsite security forces (if any are provided) or offsite law enforcement to interrupt and subdue an adversary while an attempted theft is in progress.

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 components should be considered by security managers, 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.

Draft a 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.

To be operationally effective, the security plan should be routinely reviewed, evaluated and updated.

Protect Sensitive Information

The security plan, which includes all information necessary to describe the security approach and the systems used to protect sources, and some other information related to the management of disused sources is sensitive. This information needs to be protected and should only be shared with a limited number of identified and authorised people. Procedures need to be developed to determine how this information is identified, consolidated, marked, shared, stored and handled. Secure management of sensitive information should be addressed in the security plan.

Develop an Effective and Coordinated Response Strategy

Response to an attack on your premises by an adversary is a specialist role. In some cases, it may be that onsite guards are suitably equipped and trained, but in general an operator's primary responsibility is to alert an off-site response force, usually the police or another law enforcement agency, and assist them as much as possible during their response.

In order to strengthen the cooperation with response forces, it is useful to:

- Invite them to make a visit to the site to acquaint themselves and to see the disused source store as well as everything else that is relevant to the security of radioactive materials
- Invest time in educating them about the fact that disused sources are still potentially dangerous sources and that they may be attractive to an adversary
- Periodically refresh their acquaintance with the site (as part of the security plan)

The response plan with the response forces should be periodically exercised.

Implement and Sustain Your Security System

Security systems take constant management attention and energy to ensure their continued effective operation. Security involves a wide range of activities involving the integration of people, processes and technology; the challenge for any organisation is to ensure that the right processes and procedures are in place to achieve the stated goals. Effective management of security is efficiently supported by its management under quality management systems. It is essential that you regularly conduct maintenance, training and evaluation of your security system and implement corrective actions whenever necessary. You should also ensure that best practice and operational experience are used to continuously improve your system.

OPTIONS PRIOR TO SEEKING DISPOSAL

Before disposal is selected as the end-of-life management option, several other options should be considered. Reuse and recycling may help to reduce disposal costs and reconditioning of sources could enhance both security and safety. Each of these options presents its own challenges.

Reuse

It may be possible to reuse sources that are no longer suitable for the intended purpose. As this typically involves licensing matters, it will likely require agreement from the regulatory body. This may involve transfer of ownership to another licensed enterprise (normally within the national boundary) so that the useful life of the source is extended rather than the source disposed of. This is not just a matter of postponing the inevitable need for disposal because some radionuclides can continue to be used until the source decays to below exemption levels. For example, in some cases when a cobalt-60 teletherapy source has lost some strength, perhaps after two or three half-lives, it may no longer meet the needs of a particular clinic that has high patient throughput requirements. In this case it could be re-sold to a clinic with lower patient throughput requirements. When the source eventually becomes too weak to treat patients, the teletherapy head can be removed from the equipment without extracting the source. It may then be able to be used for a different purpose; for example, the head can then be used to calibrate instruments in a calibration laboratory.

Recycling

Recycling is also sometimes an option. Radioactive contents can be removed from their capsule, reassessed and re-encapsulated to become a new source with a unique identity. However, before this option can be implemented, it invariably requires licensed users to return the source to a manufacturer or supplier who has processing facilities that can safely handle the radioactive contents. To users, the objective of return to sender will be achieved if recycling becomes possible, and it becomes a commercial decision for the manufacturer more than an end-of-life management option for the user. Consequently, recycling probably has limited relevance to many users.

The International Source Suppliers and Producers Association (ISSPA) can provide useful information about reuse and recycling of disused radioactive sources and the capabilities of their local member organisations (www.isspa.com). Through their Code of Good Practice, ISSPA members are committed to helping the user manage disused sources (e.g. returning them to the manufacturer, recycling them, and helping users access local storage facilities). Upon request, members can also provide competent technical assistance on the management of disused sources, including orphan sources.

Conditioning: Preparing Sources for Interim Storage

Radioactive sources should be prepared, or conditioned, for interim storage as quickly as possible after they become disused. Appropriate conditioning can help to reduce costs. Depending on their size and characteristics, several sources may be removed from their devices and consolidated in a shielded container specifically designed to safely store the sources and to provide suitable radiation protection. Since the devices no longer contain radioactive material, they don't need to be stored in a secure facility, thereby reducing the total volume that does need to be protected.

In some cases, the conditioning process could render sources less attractive to an adversary, which is a form of deterrence. Conditioning needs to consider how a source will be retrieved from interim storage when it is time to recycle, reuse or repackage it for permanent disposal. It would be counter-productive to condition sources in a way that renders them unsuitable for disposal: This is why the regulatory body needs to be involved in your decision making.

DISPOSAL OF DISUSED SOURCES

It is useful to understand the difference between the pragmatic and legal definitions of disposal as well as the variety of disposal options that may exist. The common sense and dictionary definition of disposal is to throw away or discard something which is considered waste. In the context of disused radioactive sources, disposal is more narrowly defined as: *to discard them to a disposal facility that is designed to hold them at the end of their lifecycle in a way that is both safe and secure.* Further, it means to dispose of them in a way that they will not be recovered in the future. This implies a purpose-designed and built repository or disposal facility.

At national level, the legal definition of disposal can be different. Where countries do not yet have any of these types of facilities, disused sources must often be placed into long-term storage. Where a store of this kind is operated by or on behalf of the State, the legal responsibilities are transferred from the user to the operator of the facility. Note that at this stage, the final disposal has not yet occurred. But the legal responsibilities have been transferred from the user. Unless this occurs, responsibility stays with the user. It is important for a business to understand this: Ongoing responsibilities for disused sources mean ongoing business risks that need to be properly managed.

If there is no facility of any kind, then the regulatory body is likely to require the user to store the disused sources on the user's own premises until a more final disposal option is available. This is likely to mean storage for a number of years. During this period, the user will remain wholly responsible legally for the safety and security of the sources, so good standards will need to be maintained over extended periods. Sustaining sufficient security over periods of years or even decades is difficult but essential.

The Options for Final Disposal of a Source

Near surface repositories may be suitable for low activity, short-lived sources. However, the specific radiological characteristics of many disused sources do not comply with the disposal acceptance criteria set up for these facilities: They constitute high, localised concentrations, or "hot spots", in the facility and could give rise to unacceptable radiation doses in the event of inadvertent human intrusion.

For long-lived disused sources which may not be suitable for disposal in a near surface repository, underground deep disposal is the preferred option. Deep geological disposal offers the highest level of isolation available among the disposal concepts currently under consideration. Another possibility is the development of a special type of national borehole disposal facility built specifically to dispose of disused radioactive sources. These options should be explored in consultation with your State regulator.

Barriers to Achieving Disposal of a Disused Source and Possible Solutions

Generally, a source lifecycle can span several years, even 30 years or more for sources containing longer-lived isotopes. Consequently, at the end of their useful life, many of the circumstances and much of the information in existence at the time of manufacture and sale may have changed. This can present various barriers to source disposal.

In 2014, the IAEA published *Management of Disused Sealed Radioactive Sources* (IAEA Nuclear Energy Series NW-T-1.3).

This detailed report, which provides reference material and technical guidance on the safe management of disused sources, is directly relevant to policy makers, users, operators of waste management facilities and regulatory bodies that are exploring options and developing strategies for long-term disposal.

If the source and the device come from different countries, it may be difficult to establish their provenance and identify the original source supplier. This can be further complicated by the fact that many sources are relatively long lived, and suppliers may go out of business or otherwise be affected by circumstances beyond their control. The result is that arrangements for returning a disused source can sometimes be invalid and the liability falls back onto the user of the source. Having suitable inventory and licensing records held by the user and regulator can help to address this issue.

When the time comes to return the disused source, availability of a suitably licensed transport container is necessary to ship the disused source. As this transaction may be many years after the initial purchase, there is a risk that the original transport package licence may have expired and does not meet current international and national regulatory requirements. Significant effort has been put forward by regulators to have suitable licensed transport packages available should this situation arise. One example of this initiative is the recent contribution to the IAEA from the United States Department of Energy's National Nuclear Security Administration of a container for transport of disused radioactive sources. As mentioned in the September 2019 press release from the IAEA:

> *The container, a model 435-B Type B(U), was designed for domestic and international transport of many types of radioactive sources and devices. It is certified to transport both very high activity sources such as teletherapy sources and irradiators, as well as sources with somewhat less activity such as those used for industrial gamma radiography and high or medium dose rate brachytherapy.*

Availability of this container will enable the IAEA to assist Member States to remove disused radioactive sources, should such assistance be required.

Another barrier that the industry faces is that many countries do not have a defined disposal pathway for radioactive sources. Consequently, the suppliers and users are unable to forecast what the disposal costs will be at the moment this disposal pathway will become available.

A further impediment may be national policy or legislative or regulatory requirements that prohibit the re-entry of sources into the State from which they originated. For example, the State may prohibit the import of radioactive waste. Therefore, it is imperative that disused sources not be designated as radioactive waste, as its re-importation may be refused. Some States distinguish between disused sources and radioactive waste so their ultimate disposition can be decided when necessary and problems with the re-importation of radioactive waste do not occur.

The costliest scenario for users is often when no prior arrangement exists and the source/device needs to be removed and decommissioned rather than exchanged for a new source or device. In such cases, users must cover the entire cost of removal and decommissioning, including packaging, administrative compliance and transportation. Furthermore, one-off shipments can be expensive, and many obstacles may need to be overcome, such as finding a suitable contractor, dealing with administrative red tape (e.g. export/import permits), finding an available certified transport package or shipment container, and locating someone who is willing to accept the source.

SUGGESTIONS FOR FURTHER READING

IAEA. (2004). *Code of Conduct on Safety and Security of Radioactive Sources.* Retrieved from www.iaea.org/publications/6956/code-of-conduct-on-the-safety-and-security-of-radioactive-sources

IAEA. (2012). *Guidance on the Import and Export of Radioactive Sources*. Retrieved from www.iaea.org/publications/8901/guidance-on-the-import-and-export-of-radioactive-sources

IAEA. (2018). *Guidance on the Management of Disused Radioactive Sources.* Retrieved from www.iaea.org/publications/13380/guidance-on-the-management-of-disused-radioactive-sources

IAEA. (2012). *TEC-DOC-1690. Review of Sealed Source Designs and Manufacturing Techniques Affecting Disused Source Management.* Retrieved from www.iaea.org/publications/8850/review-of-sealed-source-designs-and-manufacturing-techniques-affecting-disused-source-management

IAEA. (2015). STI/PUB/1667 *International Conference in Dubai, UAE 27-31 October 2013. Safety and Security of Radioactive Sources: Maintaining Continuous Global Control of Sources throughout Their Lifecycle.* Retrieved from www.iaea.org/publications/10678/safety-and-security-of-radioactive-sources-maintaining-continuous-global-control-of-sources-throughout-their-life-cycle

IAEA. (2014). *Management of Disused Sealed Radioactive Sources*. Nuclear Energy Series NW-T-1.3. Retrieved from www-pub.iaea.org/books/IAEABooks/10582/Management-of-Disused-Sealed-Radioactive-Sources

IAEA. (2012). *Radiation Protection and Safety of Radiation Sources*. International Basic Safety Standards. GSR Part 3. Retrieved from www-pub.iaea.org/MTCD/publications/PDF/Pub1578_web-57265295.pdf

IAEA. (2009). *Security of Radioactive Sources*. Nuclear Security Series No 11. Retrieved from www.iaea.org/publications/8113/security-of-radioactive-sources

IAEA. (2005). *Categorization of Radioactive Sources*. IAEA Safety Standards Series No. RS-G-1.9. Retrieved from www-pub.iaea.org/books/IAEABooks/7237/Categorization-of-Radioactive-Sources-Safety-Guide

IAEA. (1993). Revisiting Goiânia: Toward a final repository for radioactive waste. *IAEA Bulletin*.

IAEA. (1988). *The Radiological Accident in Goiânia*. Retrieved from www-pub.iaea.org/mtcd/publications/pdf/pub815_web.pdf

National Threat Initiative (NTI). Understanding Radiological Threat: Radioactive 'Dirty Bombs' are Weapons of Mass Disruption. Retrieved from www.nti.org/threats/radiological

US Nuclear Regulatory Commission. Title 10, Part 73: *Physical Protection of Plants and Materials*. 73.1: Purpose and Scope. Retrieved from www.nrc.gov/reading-rm/doc- collections/cfr/part073/part073-0001.html

WINS International Best Practice Guides. Available to WINS members at www.wins.org.

5.1 Security of High Activity Radioactive Sources
5.4 Security of Radioactive Sources Used in Medical Applications
5.7 Security of Radioactive Sources Used in Industrial Radiography and Well-Logging Applications
5.8 Security of Radioactive Sources Used in Industrial Radiation Processing

APPENDIX A

QUESTIONS TO ASSESS PERSONAL CONTRIBUTIONS TO THE MANAGEMENT OF DISUSED RADIOACTIVE SOURCES

Appendix A contains a series of questions that members of an organisation can use to evaluate the security of their disused 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 these sources within their organisation.

Questions for Chief Executives/Board of Organisations Responsible for Overseeing Radioactive Sources	
Are the Board and Executive Management aware of the disused radioactive sources in onsite storage?	☐ Yes ☐ No
Have the Board and Executive Management developed corporate policies that include disused sources in their risk management considerations?	☐ Yes ☐ No
Do the Board and Executive Management believe a credible threat exists to the disused radioactive sources in onsite storage?	☐ Yes ☐ No
Do the Board and Executive Management thoroughly understand the potential consequences and liabilities should any of the organisation's disused sources be stolen?	☐ Yes ☐ No
Have the Board and Executive Management approved and implemented a security strategy and plan that includes protection for disused radioactive sources?	☐ Yes ☐ No
Have the Board and Executive Management approved a plan for disposing of current and future disused sources?	☐ Yes ☐ No
Have the Board and Executive Management set resources aside to pay for the disposal of current and future disused sources?	☐ Yes ☐ No

Questions for Senior Managers and Supervisors	
Are you aware of radioactive sources in storage but no longer used in your organisation's operations that have been there more than a year?	☐ Yes ☐ No
Have you developed risk management strategies that align with corporate policies and specifically include disused radioactive sources in your considerations?	☐ Yes ☐ No
Do you believe a credible threat exists to the disused radioactive sources being stored by your organisation?	☐ Yes ☐ No
Do you understand the potential consequences should your organisation's disused radioactive sources be stolen?	☐ Yes ☐ No
Are you confident that effective security measures are in place to protect your organisation's disused radioactive sources? Do your continuous improvement arrangements include the security of disused sources?	☐ Yes ☐ No
Does your organisation have a plan for disposing of disused sources? Is it periodically reviewed to ensure it meets current standards and regulatory requirements?	☐ Yes ☐ No
Have sufficient resources been set aside and/or arrangements made to dispose of your current and future disused radioactive sources?	☐ Yes ☐ No
Does your organisation have a security plan that includes protection for its disused radioactive sources? Has it been tested, reviewed and revised to address any changes in the threat landscape, in the regulatory requirements, or in the activities of your organisation?	☐ Yes ☐ No
Do you know what your role and responsibilities are in the plan?	☐ Yes ☐ No
Are you aware of regulatory requirements for maintaining and disposing of disused radioactive sources?	☐ Yes ☐ No
Have you put specific arrangements in place with local law enforcement to respond to a security incident involving disused radioactive sources? Has a response exercise been conducted and "lessons learned" incorporated in the security arrangements?	☐ Yes ☐ No

Questions for Radiation Safety Officers/Security Managers	
Are you aware of high activity radioactive sources that are in storage but no longer used in your organisation's operations that have been there more than a year?	☐ Yes ☐ No
If you have any disused radioactive sources in interim storage, are they as well protected as the radioactive sources that are currently being used?	☐ Yes ☐ No
Do you specifically include these disused radioactive sources in your risk management considerations?	☐ Yes ☐ No
Do you believe a credible threat exists to the disused radioactive sources kept in your organisation?	☐ Yes ☐ No
Do you understand the potential consequences should your organisation's disused radioactive sources be stolen?	☐ Yes ☐ No
Does your organisation have a plan for disposing of disused sources?	☐ Yes ☐ No
Have sufficient resources been set aside and/or arrangements made to dispose of your current and future disused radioactive sources?	☐ Yes ☐ No
Does your organisation have a security plan that includes protection for its disused radioactive sources? Is the plan periodically reviewed and practiced to ensure it still meets regulatory requirements and other security expectations?	☐ Yes ☐ No
Are you clear on your responsibilities for the security of your organisation's disused radioactive sources?	☐ Yes ☐ No
Are you confident that an effective security system is in place to protect your organisation's disused radioactive sources? Are exercises conducted to test the effectiveness of the security arrangements?	☐ Yes ☐ No
Are you aware of regulatory requirements for maintaining and disposing of disused radioactive sources?	☐ Yes ☐ No
Have you put specific arrangements in place with local law enforcement to respond to a security incident involving disused radioactive sources? Has a security exercise been conducted and have "lessons learned" been incorporated in the security arrangements?	☐ Yes ☐ No

Questions for Staff Involved in Operations Using Radioactive Sources	
Do you believe a credible threat exists to the disused radioactive sources kept in your organisation?	☐ Yes ☐ No
Are you aware of regulatory requirements for maintaining and disposing of disused radioactive sources?	☐ Yes ☐ No
Does your organisation have a plan for disposing of disused sources? Has it been tested to make sure it is practical and will remain effective over time?	☐ Yes ☐ No
If you have any disused radioactive sources in interim storage, are they as well protected as the radioactive sources that are currently being used?	☐ Yes ☐ No
Are you clear on your role and responsibilities for the security of disused radioactive sources kept at your facility?	☐ Yes ☐ No
Are you confident that an effective security system is in place to protect your organisation's radioactive sources? Has it been tested to ensure it meets current standards?	☐ Yes ☐ No

APPENDIX B

DEFINING DIFFERENT LEVELS OF ORGANISATIONAL SUCCESS

The following chart presents five levels of effective management for the security of disused radioactive sources. Each level has its own set of characteristics. By identifying where your organisation falls on this chart, you will know what you need to do to move to the next level to improve your end-of-life management process.

Level	Characteristics
1 **RESILIENT**	Senior management has developed a corporate policy for the safe and secure management of all radioactive sources and periodically revises it to keep abreast of the most recent changes in regulatory requirements and operational matters. No high activity disused radioactive sources are stored within the organisation and on the licensed premises. Management is fully aware of the credible threats that high activity disused sources present and knowledgeable of the possible consequences resulting from a malicious act using radioactive sources. Management has established and documented a comprehensive end-of-life management strategy and process for disused sources for which the organisation is responsible. Management fully understands the organisation's potential liabilities should its disused radioactive sources be used maliciously. When the radioactive sources currently in use come to the end of their lifecycle, contractual arrangements have been put in place to return them to the supplier (or to take some other appropriate option), and sufficient resources have been set aside to fund them. The organisation has a security plan that effectively protects the disused radioactive sources awaiting disposal. The plan is periodically exercised and "lessons learned" are incorporated into it.

Level	Characteristics
2 **PROACTIVE**	Senior management has developed a corporate policy for the safe and secure management of all radioactive sources. No high activity disused radioactive sources are stored within the organisation. Management is aware of credible threats against disused sources and knowledgeable of the possible consequences should its radioactive sources be used maliciously. Management has established and documented an end-of-life management strategy and process for the organisation. Management is aware of the potential liabilities should the organisation's radioactive sources be used maliciously. The organisation has put arrangements in place and identified resources for disposing of the radioactive sources currently in use when they reach the end of their lifecycle. The organisation has a security plan that effectively protects its disused radioactive sources. The plan is regularly exercised and "lessons learned" are incorporated into it.
3 **COMPLIANT**	The organisation has some disused radioactive sources in storage, but none are Category 1 or 2 sources. Management is generally aware of credible threats against radioactive sources and somewhat knowledgeable of the possible consequences if its radioactive sources should be used maliciously. Management has established elements of an end-of-life management process for the organisation, but it is not yet fully documented. Management is generally aware of the liabilities it could face should its radioactive sources be used maliciously. Management has identified arrangements and resources for disposing of its radioactive sources when they reach the end of their lifecycle. The organisation has a security plan in place for protecting its current sources and applies it to the management of disused sources.

Level	Characteristics
4 **REACTIVE**	The organisation stores high activity (Category 1 or Category 2) radioactive sources onsite. Disposal is being considered, but resources are limited. Management is somewhat aware of credible threats to its disused radioactive sources and has some understanding of the possible consequences that could occur should its radioactive sources be used maliciously. Management has discussed the elements of an end-of-life management process, but no plans have been documented yet. Management is not aware of its liabilities should its radioactive sources be used maliciously. Management is considering arrangements for disposing of its sources when they reach the end of their lifecycle, but nothing has been put down in writing and no sources have been identified yet. The organisation has a security system that can be adapted to provide protection for disused radioactive sources in interim storage.
5 **VULNERABLE**	The organisation stores high activity radioactive sources onsite, and they have been there for several years. Management is unaware of any credible threats against its disused radioactive sources. It does not understand the possible consequences and liabilities it could face should its radioactive sources be used maliciously. Management has not had any meaningful discussions regarding the elements of an end-of-life management process. Management has put no arrangements or financing in place for disposing of its radioactive sources when they reach the end of their lifecycle. The organisation has no security plan.

ISBN: 978-3-903191-71-6

Landstrasser Hauptstrasse 1/18 A-1030, Vienna, Austria.
Tel.: +43 1 710 6519 | Email: info@wins.org | Web: www.wins.org
International NGO under the Austrian Law BGBI. Nr. 174/1992 | GZ: BMeiA-N9.8.19.12/0017-I.1/2010