WINS INTERNATIONAL BEST PRACTICE GUIDE

GROUP 5: Security of Radioactive Sources

5.3

Security of Industrial Radiography Sources

Revision 1.0

WORLD INSTITUTE FOR
NUCLEAR SECURITY

Security of Industrial Radiography Sources

A WINS International Best Practice Guide

WHY YOU SHOULD READ THIS GUIDE

The use of radioactive sources to inspect materials for hidden flaws is a valuable commercial assessment tool. Thousands of these sources are in use at any time all over the world. We know that the loss and theft of these high activity sources are a fairly common occurrence. If they are used maliciously, they have the potential to significantly harm individuals and the environment. Therefore, their security should be of great concern to users, regulators and law enforcement officials. This WINS International Best Practice Guide explains how your organisation can help to reduce the risk of theft of your industrial radiography sources and enhance their security worldwide.

About the Appendices

Appendices A and B provide a series of questions and levels of organisational competencies relating to your organisation's security of industrial radiography sources that can enable you to see how well your organisation is doing and be able to benchmark its performance. Results of this benchmarking process may indicate possible gaps in your security infrastructure and could provide you with a starting point for improving the situation.

About the Preparation of the Guide

In preparing this Guide, we have taken note of the real-life experiences of industrial radiographers and security professionals. In particular, this document borrows heavily from two regional workshops on radioactive source security for industrial radiography practices held in Sydney, Australia (September 2010)[1] and on a series of WINS workshops on the security of high activity radioactivity sources conducted in 2011 and 2012.

Wherever possible, this Guide uses the same terminology as that found in the International Atomic Energy Agency (IAEA) Nuclear Security Series[2] and Safety Series[3] publications.

---

[1] Report of the South East Asia Regional Workshop on Radioactive Source Security Level B (Industrial Radiography Practices), Sydney, Australia, 6-10 September 2010

[2] *Security of Radioactive Sources Implementing Guide*, International Atomic Energy Agency Nuclear Security Series No. 11, 2009

3 Safety Guide SSG-11, Radiation Safety in Industrial Radiography (2011).

We Welcome Your Comments

We plan to update the information in this Guide frequently 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 help or assistance with any aspect of this Guide, please email us. You can also contact us via your WINS membership portal.

WINS Contact Information

World Institute for Nuclear Security

Graben 19

AT-1010 Vienna

Austria

Email: info@wins.org

Fax: +43 (0) 1230 606089

Phone: +43 (0) 1230 606083

www.wins.org

ICNDT Contact Information

The International Committee for Non-Destructive Testing

Secretariat: The British Institute of NDT

Newton Building, St George's Avenue

Northampton, NN2 6JB

United Kingdom

Email: icndt@bindt.org

Fax: +44 (0) 1604 893861

Phone: +44 (0) 1604 893811

www.icndt.org

Dr Roger Howsley,

Executive Director, WINS

Dr J M Farley,

Chairman, ICNDT

Revision 1.0

December 2012

ISBN: 978-3-903031-58-6

WORLD INSTITUTE FOR NUCLEAR SECURITY

ICNDT INTERNATIONAL COMMITTEE FOR NON-DESTRUCTIVE TESTING

The World Organisation for NDT

WHY YOUR ORGANISATION NEEDS TO PROTECT ITS RADIOACTIVE SOURCES

Industrial radiography is the use of ionizing radiation to examine objects in a way that can't be seen otherwise. It is a major non-destructive testing (NDT) method used to determine the quality of materials and welds by using gamma rays and x-rays. The principle is similar to the use of medical x-rays to examine for broken bones. Gamma rays are emitted from radioactive material and do not need a supply of electrical power to function and, therefore, particularly adaptable for field operations. However, these sources can create considerable health and physical damage and concern if stolen and used in a malicious manner. Consequently, the overall objective of any security programme should be to minimise the likelihood of the unauthorised removal of radioactive sources and devices from company control. The physical protection and security management of these industrial radiography sources should be part of a company's relevant operational policy or programme, its plans and procedures, and communicated to all staff. Some of the factors which indicate why this is important are:

Material Attractiveness – Industrial radiography sources are attractive targets for individuals with malicious intention because of their high activity levels, ranging from ten to several hundred Curies (4 to over 50 TBq) of Iridium-192 (Ir-192), Cobalt-60 (Co-60), and Selenium-75 (Se-75). Exposure of an individual by such unshielded industrial radiography sources can cause considerable harm in a matter of minutes.

Half-Life – The half-lives of the sources are long enough to persist in the environment to cause harm and public concern: 5.3 years for Cobalt-60, 120 days for Selenium-75 and 74 days for Iridium-192.

Prevalence – Industrial radiography is an analytical technique used routinely all over the world in both urban and remote locations. At any time there are thousands of sources being used or in transit.

Portability – Industrial radiography devices containing radioactive sources are well shielded, small and lightweight: therefore easily mobile.

Locations – Industrial radiography operations are often in remote areas where local law enforcement authorities may not be readily available.

Past Security Events – There have been a number of cases of industrial radiography devices containing radioactive sources being stolen or becoming missing worldwide. The actual intent is generally not clear. However, industrial radiography radioactive sources have been central to a number of historical malicious plots involving radioactive material. These have included extortion attempts and the use of Iridium-192 as part of malicious attempts to harm individuals.

CONSIDERATIONS FOR DEVELOPING A SECURITY PROGRAMME

Your programme for securing radioactive sources should be well thought-out and diligently applied whenever you employ radioactive sources for industrial radiography operations. Besides concerns about the storage of this material and the problems in using the sources at temporary job sites, there are also significant vulnerabilities during the frequent transport of these sources between fixed locations and temporary job sites. The security concepts described in this guide can serve as a primer for developing an effective set of security measures to prevent theft[4].

These concepts, if used properly, can enhance the security of industrial radiography sources at fixed locations, during transport, and at temporary job sites. They should, to the maximum extent feasible, be adopted as prudent business practices to secure your radioactive sources against theft and other malicious acts.

It is recognized that the limited size and resources of NDT companies and the monetary value of the radiography devices may not warrant more than a modest security expenditure, but when one considers the harm to the reputation of the company and possible cleanup or other mitigation costs if there is an incident, security expenditures may be warranted.

Threat Assessment

If you recognize the security of your radioactive sources is important and may need improvement, it is then essential to know who your adversaries are and what capabilities they might have in order to determine how much security is necessary. Such an analysis of the potential threats is usually done by national authorities. It would be based on an evaluation of terrorist and criminal presence, recent security incidents, history of nuclear and radiological smuggling, criminality, corruption, etc. The output aims to describe the motivation, intentions and capabilities of credible threats which are an indication of the level of security needed. If the State has not performed a national threat assessment or defined threats applicable to industrial radiography sources, you should perform your own threat assessment to identify a baseline of potential adversary characteristics and attributes. This can be done with the assistance of security consultants and/or in coordination with local law enforcement agencies. More detailed information on this issue can be found in the WINS International Best Practice Guide, Threat Assessment (2010), and in IAEA Nuclear Security Series publication No. 10, Development, Use and Maintenance of the Design Basis Threat (2009).

Graded Approach

It is recommended that security measures be applied using a graded approach: not spending money and effort for measures that are not needed. Any security measures to be implemented should take into account the principles of risk management, including such considerations as the level of threat, the relative attractiveness of the source, and its potential to cause unacceptable consequences to the public and your organisation.

[4] It is recognized that some of the security measures described may not be permitted by national laws or regulations (e.g., background checks). If any security measure in this guide is unlawful in a particular country, adherence to national laws and regulations must take precedence.

Defence-In-Depth

Another concept to be applied when constructing an effective security system is defence-in-depth. This refers to creating a combination of multiple layers of security measures that have to be overcome to compromise security. The existence of these layers will require an adversary to avoid or defeat a number of different security measures in sequence in order to be successful. For example, an adversary might need to penetrate two or more separate barriers before gaining access to a source storage area. Moreover, it deters the adversary by adding uncertainty, requiring different techniques and tools, and creating additional steps. A layered defence approach adds to a system's overall reliability by eliminating dependency on one security measure, creating vital redundancy, which protects against a single point of failure.

IMPLEMENTING A GOOD SECURITY PROGRAMME

When these initial considerations are understood, the actual design of a security programme can be initiated. This guide separates the suggested approach into two sets of elements: **protective elements** and **management measures**.

How your programme is actually structured is up to your organisation, but some aspects of these elements will, of necessity, have to be either explicitly or implicitly addressed in a comprehensive security programme. They are provided below and then followed by a set of best practices which demonstrate at a more detailed level how they can be implemented operationally.

It is not expected that small or medium sized companies immediately adopt the measures recommended in this guide. These measures can also be seen as a target for improvement as changes are made to company procedures and facilities. Some suggestions, such as enhancing security culture, including security awareness training can start immediately and with little cost.

PROTECTIVE ELEMENTS

Good security is one of balanced protection: a concept of equivalent security functions that provides adequate protection against all threats along all possible pathways. Thus the security system should incorporate a number of protective elements described below which, when employed correctly, will establish the web of defences to combat an adversary: **Deterrence, Access Control, Detection, Assessment, Delay** and **Response**. This is not necessarily a sequential list of measures since physical protection functions do not always follow such a chronological order: rather a security system is made of multiple combinations of these functions.

Deterrence

When implementing a security programme, it is useful to have certain protection elements visible to potential adversaries, e.g. fence, lighting, regular security patrols, signs, and guards properly attired. It is a good tactic to demonstrate a security profile that appears robust, so that an adversary will be reluctant to attack.

Access Control

The objective of access control is to ensure that only appropriate users have access to a facility and to radioactive sources used by your company. There is a wide array of measures that you can apply to help secure access: procedural, electronic and physical. For example, it can include such measures as validating the suitability of an individual, restricting entry of individuals and vehicles to a facility, controlling keys to storage locations, radiography source devices and containers. Access control should be designed to minimize the impact on individuals and interference with operations. Access control measures should also be applied to vehicles and goods entering or leaving your premises.

Detection

Early detection is a key component to help any response force interrupt an adversary. Normally detection systems are combined with an assessment system since there is no meaningful detection without knowing what the alarm really means. Facilities are usually designed to limit the number of adversary pathways to the source storage areas which allows for the effective use of detection and assessment equipment.

Ideally, detection systems should be properly designed and installed to incorporate complementary technologies so that the adversary must use a variety of defeat methods. Detection systems are also designed to have a low nuisance and false alarm rate with a high probability of detection and able to detect tampering by the adversary.

Care then would be taken to make the system reliable and robust for the operating environment. Any system should be maintained and its effectiveness periodically verified through a performance testing programme.

Assessment

Personnel should be trained to verify the authenticity of an alarm occurrence and be capable of initiating a response. When affordable, closed circuit television (CCTV) monitoring of selected locations can be an effective means of alarm assessment. To be considered an assessment tool, CCTV should be available twenty-four hours a day and monitored at all times.

Assessment should take place in a protected location that is not vulnerable to intruders and assessment personnel, such as on-site guards or operations personnel, should have a reliable means to summon help immediately, e.g., duress buttons, radios, etc. It should also be noted that common practice is to save CCTV recordings for investigative purposes and insider theft deterrence.

Delay

An adversary can be delayed by the use of barriers to provide sufficient time for the assessment of and response to criminal or malicious acts. The location of delay elements is important in a physical protection system.

It is usually less expensive to place barriers closer to the target being protected when trying to protect against the theft of radioactive sources. When sabotage is the principal concern, delay elements should be placed as far from the target being protected as possible to allow response forces more time to interrupt the adversary actions.

Several different delay barriers are usually applied in the protection of radioactive sources, forcing the adversary to bring a variety of tools to defeat each delay element. Integrating these delays into the facility design is a help in minimizing the effect they have on safety features. It is also a good idea to take advantage of design features associated with the facility. It is very important that sufficient delay is provided after detection so that response personnel can interrupt the adversary. Delay measures are part of the physical protection system and will not be effective without detection and assessment.

Response

It is important to develop a plan to respond to a security incident along with procedures to define roles and responsibilities among operator staff and people who would respond (security contractor, law enforcement) either at the fixed location, during transport or at a temporary job site.

When on-site guards are used, they should be properly equipped and trained and most importantly, they should be part of a trustworthiness/reliability programme. Since communications are always a vital element of any response, there is a need to have reliable and diverse communications. Then, to assure that the response plan is appropriate and to validate response force readiness, exercises should be conducted periodically.

MANAGEMENT ELEMENTS

In addition to these protective elements, the security system needs to integrate people and procedures, as well as the continuous training of radiographers, the exercise of security measures and the protection of information and other related management measures.

Procedural Development

The individual responsible for the security of industrial radiography sources should have the needed authority and accountability to effectively manage the security system, and should revise existing procedures or develop new ones for the following:

- Operational procedures;
- Access control procedures;
- Insider protection programme to include human reliability assessments and such other measures as access control, two-person rule, key and lock controls;
- Response plans in coordination with the appropriate authorities;
- Conducting periodic tests or exercises to validate response force readiness;
- Preventive maintenance programme for the proper operation of the security equipment;
- Performance testing for the security system by the facility staff to support continued effective operation of the system; and
- Procedures for the protection and retention of security-related documents and sensitive information.

Written procedures should describe all the existing security measures and, where necessary, revised to include the security responsibilities of staff at the fixed location, temporary job sites, and in transport.

Your company should develop a security plan to describe the overall security measures in place to protect the radioactive sources. (Guidance on the contents of a security plan is included at the end of this part of the guide.) Procedures should be developed to implement, test, periodically review and revise that security plan.

Procedures and arrangements should be established to perform human reliability assessments. Background checks, reference checks, trustworthiness determinations, etc., are normally implemented as allowed by company polices and national laws. If a check cannot be performed due to legal restrictions or lack of available information, the company should consider these limitations in their actions to mitigate possible insider threats.

Security Awareness and Training for Staff

You should develop a listing of required security related training topics, and the personnel who should obtain the identified training. A primary purpose of training should be the development of skills and competencies of the staff necessary to meet the requirements of their work and job descriptions. Among others, this training could cover the operation of security equipment and the implementation of security procedures for the protection of radioactive sources (e.g., access control, material surveillance, response actions).

The security equipment contractor or other specialised companies should provide on-going security training to radiographers, especially those who take sources to temporary job sites, use them in the field and are responsible for their security at temporary storage areas when away from the company and a fixed storage location. It is good practice to conduct periodic security awareness and procedure training along with safety training.

Consideration should also be given to additional training topics such as human factors impacting security performance and security culture[5], which may be developed in-house or by a qualified third party.

Alarm Monitoring

The intrusion detection system and other alarms should be monitored on-site and, as applicable, by an off-site alarm monitoring station.

The off-site function can be performed by a variety of entities to include commercial central alarm stations, company operations centres, police stations, etc. The intent of the off-site alarm monitoring is to avoid a single point of failure that depends on on-site personnel to initiate a response.

[5] For further discussion of security cultures, see WINS International Best Practice Guide, *Security Culture*.

Equipment Performance

A regular performance testing programme, both internally and in conjunction with the security equipment contractor, is a normal practice to test the effectiveness and reliability of equipment, people, and procedures.

Maintenance

It is important to develop and implement a security equipment maintenance programme, including functional testing and preventative actions. Security equipment contractors normally provide warranty, maintenance, testing, and upgrade services for the equipment installed.

Information Security

Where it is necessary to limit access to security sensitive information to those persons who have a need to know, specific procedures should be developed. This includes protection of information about the material and operations, transport timing and routes, and specific information about security measures.

Actions to be taken in Case of Loss or Theft of a Radiography Device

In the event of a loss or theft of a radiography device, it is critical to provide law enforcement authorities and other relevant organisations with reliable information on the circumstances of the incident and details about the missing device(s). To facilitate this process, it is suggested that information about your devices and contained radioactive sources be gathered into a single file and kept securely as both a hard copy and an electronic file. This, for example, should include information enabling the positive identification of the equipment, such as, any wording on the device, size, weight, serial number and pictures of the device.

BEST PRACTICES FOR THE SECURITY OF INDUSTRIAL RADIOGRAPHY SOURCES

The following set of practices demonstrates at a more detailed level how the physical and management elements described above could be implemented operationally.

FIXED LOCATIONS (MAIN STORAGE/BUNKER)

- **Store radiography sources in a dedicated storage area.**

  The walls of the storage area should be of robust design and the number of access points (doors; windows…) to the area should be minimised and hardened (locks, grids…).

- **Store radiography devices in separate locked compartments (e.g., a safe) within the storage area.**

  Such measure provides an additional layer of protection after access in the storage room. It prevents a direct and easy access to multiple radiography devices if access control to the storage room is compromised.

- **Implement a two-person rule access control system for radiography source storage areas containing multiple radiography devices.**

  To gain access to the storage area, this access control system requires that two authorized employees be present and that each employee possesses one key/card/code to open their assigned delay element. This measure provides an additional layer of defence to background checks or an evaluation of trustworthiness/reliability and further lessens the risk of an insider committing theft or diversion of a radiography sources.

  In instances where a strict two-person rule cannot be implemented for operational reasons, such as a lack of personnel, the company should institute alternative physical and management elements that will mitigate the insider threat, and in particular track who had access to the storage area or to the safe.

- **Store keys and other access cards into security boxes, such as key safes.**

  Security boxes should be located in protected locations (e.g., rooms with intrusion detection; locked areas; not accessible by public).

- **Track the movement of sources in and out of storage.**

  Movement of sources should be recorded in a readily available log book. Procedures should be developed to ensure that movement of sources have been authorised.

- **Source changers, empty containers and handling tools should be stored and secured separately from the sources** to reduce the likelihood that these items could be used to facilitate the diversion of a source.

- **Ensure reliable intrusion detection in the storage.**

  Install an intrusion detection system in the storage area. The area should be equipped with at least 2 motion detectors and the doors and other openings leading to the source storage location should be equipped with Balanced Magnetic Switches (BMS) or other devices to detect their opening.

  Detections should activate a local siren and strobe light to provide an alarm indication in the vicinity of the source storage location. It is common that audible alarms exceed 100 decibels.

  When a large number of devices are stored, the intrusion detection alarms should also be reported to an alarm monitoring station.

  The main electrical power source for the intrusion detection system should be supported by an auxiliary system capable of providing power for at least 48 hours.

  Security equipment (intrusion detection system, locks, security doors…) installed in the facility should comply with industrial security standards.

  It is good practice to consider extending the intrusion detection system and other security provisions to all areas of your facilities where sources can temporarily present a risk.

- **Provide the staff with means to send an alarm to alert in case of a security incident.**

  The intent of this measure is to allow personnel accessing the source storage area to summon a response because the detection system would have been deactivated to allow access.

  It is most important to install a duress signal in or near the source storage and equipment loading areas. Whenever practical, the use of mobile alert devices should be considered.

- **For large inventories, new facilities or high threat environments, provide CCTV coverage of source storage and other locations where sources can temporarily present a risk.**

  The CCTV system should be adapted to the specific conditions of the facility. It is common that CCTV systems are functional under artificial and low level lighting conditions. Outdoor cameras should be kept in appropriate environmental housings.

  CCTV footage should provide a clear and suitable image for assessment and evidentiary purposes, and should be recorded by a digital video recorder with a minimum of 96 hours of recordable storage capacity. The digital video recorder response must be rapid enough to record any intrusion.

- **Provide basic security awareness training** to individual(s) responsible for the security of sources and other selected staff (such as radiographers, drivers…) as appropriate.

- As much as possible, **do reliability checks on key staff.**

  Based on national legislation and practices, reliability checks may include verification of criminal records, credit situation, job references, etc.

- **Draft a security plan** that gathers together all security related information (roles and responsibilities, organisation, measures, procedures…).

- **The security plan should include response arrangements, and roles, responsibilities and capabilities of on-site and off-site organisations in case of a security incident.**

- **Determine the actual status of security arrangements.**

  Periodically schedule drills and exercises (both tabletop and field exercises) to evaluate the adequacy of security and response procedures and arrangements and determine the status of their implementation.

INDUSTRIAL RADIOGRAPHY SOURCES BEING TRANSPORTED BY COMPANY-OWNED VEHICLE

- **Install an alarm system on the vehicle** to detect an intruder attempting to enter the vehicle.

  At a minimum, a local audible alarm should be activated in case of intrusion. Preferably, the vehicle should be equipped with an alarm system capable of sending a signal (e.g., cellular/radio, etc.) to the driver and other selected remote staff/locations.

- **Equip vehicle with anti-theft device.**

  Consider the installation of a remote engine cut-off capability (if allowed by company policies and relevant safety authorities).

- **Track the vehicle.**

  Consider the installation of a tracking device reporting the position of the vehicle.

- **Install a high security lock on the door to the cargo compartment.**

  Whenever possible, the lock should have a shielded shackle to prevent the cutting of the lock. To ensure balanced security, the cargo compartment walls and hinges of door should provide at least equal delay as the door high security lock.

- **Install a high security lock on the radiography device transport container.**

  To ensure balanced security the transport container should be tied down to the vehicle and its construction should provide at least equal delay as the high security lock.

- When practical, **enforce a two-person rule for access to the radiography device.**

  One way to do this is to provide one individual with the key to the vehicle cargo compartment and another one with the key of the source transport container.

  In instances where a strict two-person rule cannot be implemented (e.g., operational reasons), the company should demonstrate that they have instituted alternative physical or procedural measures that provide reasonable assurance against an insider threat during transportation.

- To the extent possible, **drivers and/or other transport staff should maintain constant surveillance of the vehicle.**

  Periods when the vehicle is left unattended should be kept to the strict minimum. Whenever possible, the vehicle should be parked in areas which are continuously under surveillance (e.g., parking garages with attendants). When left unattended, vehicles should be locked and alarms activated.

- **Provide driver(s) and other transport staff with means of communication** such as cell phones, radios, satellite phones.

  Redundant means of communication would be useful to compensate for the lack of coverage of any one technology. In the absence of any reliable means of communications due to lack of infrastructure or remoteness of location, the company should implement pre-planned periodic checks for the timely detection of any incident.

  If possible, provide mobile duress alarms for use by the drivers in transit. The buttons should provide an alarm indication at the company alarm station (if applicable) and off-site alarm station (such as security contractor monitoring stations).

- In areas where there is a high level of threat, **conduct route planning** to identify potential threats and existing response authorities (police, security contractors…) in order to select the most appropriate route and alternates.

When possible, have pre-arranged agreements with appropriate law enforcement for assistance in response to an actual or attempted theft of radiography sources. If extensive preplanning is not realistic, then at a minimum, the company should develop a list of the appropriate authorities to contact in the jurisdictions where the transports are occurring.

- **Provide drivers and other transport staff with written instructions** to be implemented in case of security related event.

  These instructions should include, among others, locations of authorised stops (eating, fuelling, rest, long term parking…), operation of the alarm system, access procedure to the cargo compartment, actions to be taken in case of theft of the vehicle, phone numbers of key company staff and relevant law enforcement agencies.

  These instructions should be developed in coordination with other applicable transport instructions (operations, safety…).

- As much as possible, **do reliability checks on drivers and other transport staff.**

- **Coordinate with the client on the arrival and placement of sources at field locations.**

  Transport staff should also confirm source arrival to their management.

- **Draft a security plan** that gathers together all transport security related information (roles and responsibilities, organisation, measures, procedures…).

- **Determine the actual status of security arrangements**

  Periodically schedule drills and exercises to evaluate the adequacy of security and response procedures and arrangements and determine the status of their implementation.

TRANSPORT BY A THIRD-PARTY CONTRACTOR

- **The contract with the transport company should require security measures consistent with those detailed above (Transport by company-owned vehicles).** In particular, the contract should cover measures to keep control of radiography sources (including detection and delay measures), route planning, communications, confirmation of delivery and procedures in case of an incident.

  The transport company should be **licensed and certified to transport** the radioactive material sources and the drivers should be adequately trained for their responsibilities.

- Whenever possible, **schedule company personnel to be present when sources arrive** at the destination.

- **Request copies of route planning documentation** and, where possible, request periodic information on the position of the vehicle.

- **Record transport information** prior to shipment (license plate numbers, make/model of vehicle, driver's name, etc.) and after the transport (copy of transport documents, confirmation of delivery…).

TEMPORARY JOB SITES

- **Radiography devices should be kept under constant surveillance by a radiographer or radiographer's assistant when not stored in the transport vehicle or in secure temporary storage.**

  Surveillance could be performed either by visual or electronic surveillance.

  When constant surveillance is not practical, the presence of the radiography device should be checked periodically by company personnel or personnel assigned by the site operator (if applicable), such as the guard force. It is important to note that this will result in a delay to detection.

- **Radiography devices not in use should be kept in the transport vehicle or in secure temporary storage.**

  The temporary storage room (or area) should have some form of access control and intrusion detection that would provide an alarm annunciation to company personnel on site.

  Preferably, portable radiography devices should be stored inside an additional container designed to minimize theft opportunities (locked and weighted down; tied down to the floor…).

  When possible, keys for accessing the storage locations and storage containers should be separated between different employees.

  In the absence of a formal agreement with the customer, primary responsibility for control of the radiography device rests with the radiography company.

- **Provide radiographers and other company staff with means of communication** such as cell phones, radios, satellite phones.

  If possible, provide means of communication equipped with mobile duress alarms. These devices should provide an alarm indication at a permanently staffed location (either at temporary job sites, company headquarters or private security monitoring stations).

- In locations where there is a high level of threat, **identify the responsible person for security at the field location and review security arrangements with appropriate site personnel.**

  The briefing should cover, among others, possible consequences in case of loss of control of the radiography sources and basic procedures to be implemented in case of attempted or actual theft.

EXAMPLE OUTLINE FOR A SECURITY PLAN

Chapter I Introduction

I.1 Background

I.2 Objective

Chapter II Organisation of the Company for Managing Security

II.1 Roles and Responsibilities for Security

II.2 National Regulatory Compliance Requirements

II.3 Training Programme

II.4 Performance Testing Programme

II.5 Maintenance Programme

II.6 Budget and Resource Planning

II.7 Background Checks

II.8 Information Protection

Chapter III Facility Description

III.1 Isotopes and Quantities of Concern / Categorization of Radioactive Sources

III.2 Description of Facility and Surrounding Environment

III.3 Security System Design

III.3.1 Threat Assessment

III.3.2 Security Assessment Methodology

III.3.3 Definition of Security Layers

III.3.4 Access Control Measures

III.3.5 Description of Technical Barriers

Chapter IV Operational Security Procedures

IV.1 Routine, Off Shift, and Emergency Operations

IV.2 Opening and Closing of Facility

IV.3 Key and Lock Control Measures

IV.4 Source Accounting Measures

Chapter V Response Planning

V.1 Communications Plan

V.2 Emergency Response and Contingency Planning

V.3 Security Event Reporting

APPENDICES

APPENDIX A - QUESTIONS TO ASSESS PERSONAL CONTRIBUTIONS TO THE SECURITY OF INDUSTRIAL RADIOGRAPHY RADIOACTIVE SOURCES

APPENDIX B - DEFINING DIFFERENT LEVELS OF ORGANISATIONAL SUCCESS

APPENDIX A

QUESTIONS TO ASSESS PERSONAL CONTRIBUTIONS TO THE SECURITY OF INDUSTRIAL RADIOGRAPHY RADIOACTIVE SOURCES

Appendix A contains a series of questions that members of an organisation can use to evaluate the security of their industrial radiography 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 THE EXECUTIVE MANAGERS6 OF AN INDUSTRIAL RADIOGRAPHY COMPANY

Do you believe that there is a possibility that your radioactive sources could be stolen and a special effort is required to prevent that?	☐ Yes ☐ No
Does the Owner(s)/Board of Directors routinely consider the various aspects of security of industrial radiography sources?	☐ Yes ☐ No
Are you aware if there has been an evaluation of the threats to your radioactive sources?	☐ Yes ☐ No
Are you aware of your potential liabilities in case of malicious use of your sources?	☐ Yes ☐ No
Have you approved standards or policies for the security of sources during the various operations involving them (at company location, at temporary job site and during transportation)?	☐ Yes ☐ No
Have you approved a training programme for individuals involved in the security of your industrial radiography sources?	☐ Yes ☐ No

[6] Executive managers can be a Board of Directors, owner(s) or others who have the final responsibility for a company's actions.

QUESTIONS FOR SENIOR MANAGERS AND SUPERVISORS OF AN INDUSTRIAL RADIOGRAPHY COMPANY

Do you believe that there is a possibility that your radioactive sources could be stolen and a special effort is required to prevent that?	☐ Yes ☐ No
Do you conduct periodic meetings (either separately or during safety or operational meetings) with your staff on security threats or requirements?	☐ Yes ☐ No
Do you have security procedures for protecting sources at your premises?	☐ Yes ☐ No
Do you have security response arrangements (police, security vendor…) in place?	☐ Yes ☐ No
Do you perform background checks of radiographers, drivers and other key staff?	☐ Yes ☐ No
Is there a regular training programme for individuals involved in the security of industrial radiography sources?	☐ Yes ☐ No
Do you have specific security features and procedures for vehicles transporting sources (e.g. route planning, pre-arranged plans with law enforcement, vetting of drivers, exercises, delivery confirmation…)?	☐ Yes ☐ No
Do you consider security arrangements at temporary job sites as effective as at company location and during transport?	☐ Yes ☐ No
Do you periodically exercise your security arrangements and procedures?	☐ Yes ☐ No

QUESTIONS FOR INDUSTRIAL RADIOGRAPHY FIELD STAFF

Do you believe that there is a credible threat to the industrial radiography sources you use?	☐ Yes ☐ No
Are you implementing security procedures to protect your sources against theft?	☐ Yes ☐ No
Have you received written instructions in the event of a security incident?	☐ Yes ☐ No
Have you received training for implementing the security procedures? Do you consider it adequate?	☐ Yes ☐ No
Are you confident with the level of security for your sources?	☐ Yes ☐ No
Have you been involved in a response exercise for a security event involving your sources?	☐ Yes ☐ No
Is the level of security during transport as effective as at company location?	☐ Yes ☐ No
Is the level of security at job sites as effective as at company location?	☐ Yes ☐ No
If you observe any suspicious behaviour, in particular at job sites, do you know who to report it to or what to do?	☐ Yes ☐ No

APPENDIX B

DEFINING DIFFERENT LEVELS OF ORGANISATIONAL SUCCESS

The following chart presents five levels of security of industrial radiography sources each with 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 the security of these sources.

LEVEL	CHARACTERISTICS
1 **WORLD CLASS**	a) Management is aware of the credible threats to the sources and knowledgeable of the possible consequences resulting from malicious act. b) The organisation has a detailed security plan which clearly delineates the authority and accountability of security management. c) An extensive vetting programme is in place which includes background checks, reference checks, trustworthiness determinations, as allowed by company polices and national laws. d) A two-person rule for access to the sources at the base, in transport and at the site has been implemented and operates effectively. e) A response plan has been developed and contacts are made to the local law enforcement authorities to make them aware of the sources and support needed in a security emergency. Response exercises are conducted periodically, f) A training programme is in place to provide security awareness to individuals responsible for the sources or working with them. Refresher training is provided at least every 2-3 years. The competency of radiographers for their responsibilities is assured.
2 **HIGHLY EFFECTIVE**	a) Management is aware of possible threats to the sources and has a grasp of the possible consequences resulting from malicious act. b) The organisation has a security plan which reflects the authority and accountability of security management. c) Vetting is in place which includes reference checks which are as allowed by company polices and national laws. d) A two-person rule policy is in place but not always fully implemented in practice. e) Contacts are made to the local law enforcement authorities to make them aware of the sources and support needed in an emergency. Response exercises are conducted occasionally. f) A training programme is conducted to provide security awareness to individuals responsible for the sources or working with them. The competency of radiographers for their responsibilities is considered.

3 **GOOD**	a) Management is aware that it is responsible for securing the industrial radiography sources. b) The organisation has operational procedures which delineates the management accountability for security. c) A vetting programme has been developed but not fully implemented because of slow or inadequate responses d) A two-person rule for access to the sources at the fixed Location but not always applied at other locations and in transport. e) Contacts have been made to the local law enforcement authorities about the possible need for support in an emergency. Response exercises have not been conducted. f) Security awareness training is provided to individuals responsible for the sources in a structured manner.
4 **DEVELOPING**	a) Management is aware that it is responsible for assuring the security of the industrial radiography sources. b) Sources are locked most of the time but occasionally when inconvenient to do so, they may go unattended. c) There is no vetting of personnel who handle the industrial radiography sources. The two-person rule is applied where convenient. d) There is little concern about incident planning but contacts have been made with local law enforcement authorities e) Some security awareness and procedures training is conducted but not on a structured basis.
5 **INEFFECTIVE**	a) The organisation does not have a security plan and is not clear who has the responsibility for assuring the security of the industrial radiography sources. b) Sources are routinely left unattended, particularly during transport. c) There is no vetting of personnel who handle the industrial radiography sources and a two-person rule is not generally applied. d) There is no response plan in the event of a security incident involving the sources and, consequently, there are no response exercises. e) There is little training on security awareness or procedures for individuals responsible for the sources or working with them.

WINS Best Practice Guides

Group 1: NUCLEAR SECURITY PROGRAMME ORGANISATION

1.1 Effective Security Regulation and Implementation
1.2 Legal Accountability and Liability for Nuclear Security
1.3 Security Governance
1.4 Nuclear Security Culture
1.5 Performance Metrics
1.6 Making Security Efficient

Group 2: MANAGING AND COMMUNICATING SECURITY INFORMATION

2.1 Threat Assessment
2.2 Managing Security Threat Information
2.3 Information Security for Operators: Challenges and Opportunities
2.4 Communicating Security Information: Striking a Balance
2.5 Engaging with External Stakeholders on Nuclear Security

Group 3: PEOPLE IN NUCLEAR SECURITY

3.1 Developing Competency Frameworks for Managers with Nuclear Security Accountabilities
3.2 Human Reliability as a Factor in Nuclear Security
3.3 Nuclear Security for Scientists and Engineers
3.4 Managing Internal Threats
3.5 Working Effectively with External Response Forces
3.6 Nuclear Security Guard Recruitment and Selection
3.7 Guard Force Training and Motivation
3.8 Effective Management and Deployment of Armed Guard Forces

Group 4: IMPLEMENTING SECURITY MEASURES

4.1 Security by Design
4.2 An Integrated Approach to Nuclear Safety and Nuclear Security
4.3 Security of IT and IC Systems at Nuclear Facilities
4.4 Material Control and Accountancy in Support of Nuclear Security
4.5 Learning from Operating Experience
4.6 Security Exercises
4.7 Modelling and Simulation for Nuclear Security
4.8 Electronic Tracking for the Transport of Nuclear and other Radioactive Materials
4.9 Security Equipment Maintenance
4.10 Nuclear Transport Security

Group 5: SECURITY OF RADIOACTIVE SOURCES

5.1 Security of High Activity Radioactive Sources
5.2 Security of Well Logging Radioactive Sources
5.3 Security of Industrial Radiography Sources
5.4 Security of Radioactive Sources Used in Medical Applications

---

For further information on translated guides please go to WINS website **www.wins.org**

ISBN: 978-3-903031-58-6

WORLD INSTITUTE FOR NUCLEAR SECURITY

 Graben 19, A-1010 Vienna (Austria)
Tel.: +43 1 23060 6083 | Fax: +43 1 23060 6089 | Email: info@wins.org | Internet: www.wins.org
International NGO under the Austrian Law BGBl. Nr. 174/1992 | GZ: BMeiA-N9.8.19.12/0017-I.1/2010