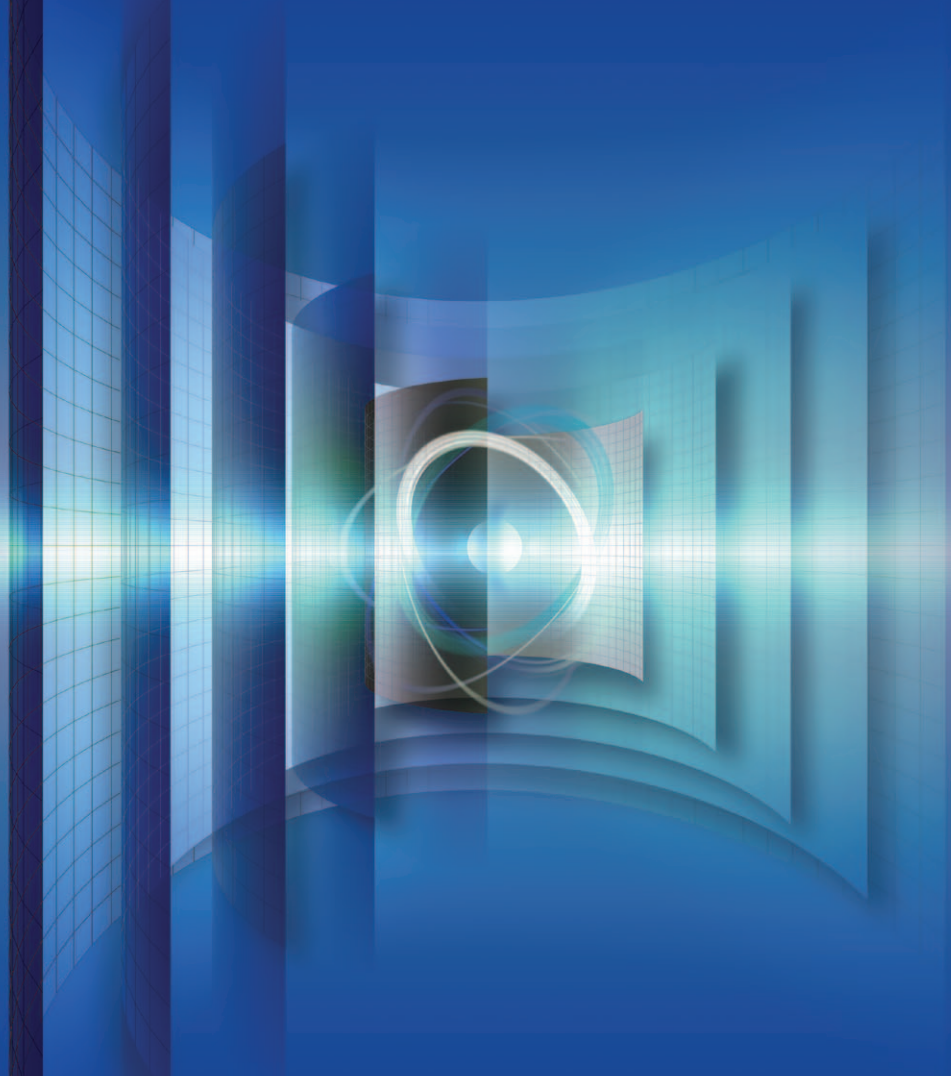
IAEA Nuclear Security Series No. 11

Implementing Guide

Security of Radioactive Sources



IAEA
International Atomic Energy Agency

SECURITY OF RADIOACTIVE SOURCES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 11

SECURITY OF RADIOACTIVE SOURCES

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

COPYRIGHT NOTICE

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
May 2009
STI/PUB/1387

IAEA Library Cataloguing in Publication Data

Security of radioactive sources : implementing guide. — Vienna : International Atomic Energy Agency, 2009.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816-9317 ; no. 11)
STI/PUB/1387
ISBN 978-92-0-102609-5
Includes bibliographical references.

1. Radiation sources — Safety measures. 2. Radiation sources — Security measures. I. International Atomic Energy Agency. II. Series.

IAEAL 09–00573

FOREWORD

In response to a resolution by the IAEA General Conference in September 2002, the IAEA has adopted an integrated approach to protection against nuclear terrorism. This approach coordinates IAEA activities concerned with the physical protection of nuclear material and nuclear installations, nuclear material accountancy, detection and response to trafficking in nuclear and other radioactive material, the security of radioactive sources, the security in the transport of nuclear and other radioactive material, emergency response and emergency preparedness measures in Member States and at the IAEA, and the promotion of adherence by States to relevant international instruments. The IAEA also helps to identify threats and vulnerabilities related to the security of nuclear and other radioactive material. However, it is the responsibility of States to provide for the physical protection of nuclear and other radioactive material and their associated facilities, to ensure the security of such material, including in transport, and to combat illicit trafficking and the inadvertent movement of such material.

Radioactive sources provide great benefit to humanity, primarily through their use in agriculture, industry, medicine, and research, and the vast majority are used in well regulated environments. However, control has been lost over a small fraction of those sources, sometimes resulting in accidents of which some had serious consequences.

Today, there is a growing concern that terrorist or criminal groups could gain access to high activity radioactive sources and use the sources maliciously. Consequently, there has been a global trend towards increased control, accounting and security of radioactive sources to prevent their malicious use and any potential associated consequences.

The Code of Conduct on the Safety and Security of Radioactive Sources is one example of this global trend. It was revised in 2003 to contain stronger security principles, including the recommendation for each State to define its domestic threat and assess its vulnerability with regard to this threat for the variety of sources within its territory. Additionally, several important international conferences have been convened on this topic and concluded that the security of radioactive sources should be a global priority and that efforts should increase to combat the illicit trafficking of radioactive sources.

This publication provides guidance that can be used by regulatory authorities when establishing national requirements for the security of radioactive sources.

The preparation of this publication in the IAEA Nuclear Security Series has involved extensive consultations with Member States, including an open-ended technical meeting in Vienna in May 2006. As a final step, the draft was

circulated to all Member States to solicit further comments and suggestions before publication.

EDITORIAL NOTE

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

This publication offers guidance for implementing security measures on radioactive sources. It also provides advice on implementing security related provisions in the Code of Conduct on the Safety and Security of Radioactive Sources [1] (hereafter referred to as the 'Code of Conduct') (see the Definitions for explanations of the terms in this publication).

This Implementing Guide, while replacing Security of Radioactive Sources — Interim Guidance for Comment (IAEA-TECDOC-1355) [2], takes account of the overall security approach established in that publication which some States may have used as a reference in devising their current security regimes. This publication has been harmonized with the IAEA's Categorization of Radioactive Sources [3] and proposes a graded approach to security using a set of security levels, and the security functions of deterrence, detection, delay, response and security management.

This publication should be read in conjunction with the Code of Conduct [1], the Categorization of Radioactive Sources [3], the Safety of Radiation Generators and Sealed Radioactive Sources [4], the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [5], and the IAEA Fundamental Safety Principles [6].

Finally, this guide recognizes that there should be a balance between managing sources securely while still enabling them to be used safely by authorized personnel. Since radioactive sources are an integral and critical tool in the world's health care, manufacturing, research and quality control industries, care needs to be taken to ensure that the many beneficial uses of sources are not unduly hindered. The challenge for the regulatory body, users and other stakeholders is to find the correct point of balance.

1.2. OBJECTIVE

This publication is intended for use by States in formulating security policy for radioactive sources and by regulatory bodies in developing regulatory requirements that are consistent with the Code of Conduct. It will also assist State parties to fulfil certain obligations under the International Convention for the Suppression of Acts of Nuclear Terrorism [7]. It may also be useful to operators managing radioactive sources in developing their security programmes.

1.3. SCOPE

This publication includes guidance and recommended measures for the prevention of, detection of, and response to malicious acts involving radioactive sources. It will also help towards preventing the loss of control of such sources. It does not apply to nuclear material as defined in the Convention on the Physical Protection of Nuclear Material and the Amendment thereto [8], except for sources incorporating plutonium-239.

While this guide does not specifically address the security of unsealed radioactive material, a State may choose to apply the security concepts and measures outlined in this guide to such material.

This publication recommends that security measures be applied to radioactive sources in manufacture, use and short term or long term storage (see the Definitions).

This guide recommends that security measures be applied on a graded basis, taking into account the current evaluation of the threat, the relative attractiveness of the source, and the potential consequences resulting from malicious use. The requisite level of security is achieved through a combination of deterrence, detection, delay, response and security management.

States may decide that some or all sources are at greater or lesser risk than the basis on which this guide was written. In such cases States will need to have the flexibility to vary the security measures they require, compared with those that are recommended here. When doing this, States will need to remain within the overall structure of this guide as much as possible.

This guide does not include recommendations on emergency preparedness and response, intervention, or the remediation of contaminated areas. Such guidance is available in other IAEA publications [5, 9, 10]. Guidance on protecting people against radiation in the aftermath of an attack is given by the International Commission on Radiological Protection [11].

Finally, this publication does not deal with radioactive material, including radioactive sources, while in transport. Such guidance, including that for third party shippers, is given in Ref. [12].

2. RESPONSIBILITIES OF THE STATE AND OPERATOR

2.1. INTRODUCTION

The Code of Conduct [1] recognizes that an effective national system of regulatory control underpins the safety and security of radioactive sources in a State. This section provides further guidance on the responsibilities of the State and the operator with regard to the security of radioactive sources.

2.2. STATE

Every State will need to define its domestic threat (see Section 3.8.1). This process needs to begin with a national threat assessment, which is an analysis that documents — at a national level — the credible motivations, intentions and capabilities of potential adversaries that could cause harm through the sabotage of a facility or the unauthorized removal of a radioactive source for malicious purposes. Guidance on this topic is discussed in detail in Ref. [13].

Every State will need to take the appropriate measures to ensure that radioactive sources within its territory, or under its jurisdiction or control, are securely protected during and at the end of their useful lives. This includes the promotion of a security culture with regard to radioactive sources and adequate education and training of regulators and operators.

States will need to have an effective national legislative and regulatory infrastructure in place to govern the security of radioactive sources, which:

— Prescribes and assigns governmental responsibilities to relevant bodies including an independent regulatory body to establish, implement, and maintain a regime that ensures the security of radioactive sources;
— Establishes security requirements for radioactive sources and includes a system of evaluation, licensing, and enforcement or other procedures to grant authorizations;
— Places the prime responsibility for the security of radioactive sources on the operators;
— Provides for measures to reduce the likelihood of the attempt of malicious acts;
— Provides for measures that mitigate/minimize the consequences of malicious acts involving radioactive sources;

— Establishes punishable offences covering malicious acts involving radioactive sources;

The implementation and operation of the legislative and regulatory infrastructure for the security of radioactive sources rely on the effective cooperation between the various bodies assigned governmental responsibilities. Typically, these bodies are likely to include a State's regulatory body, intelligence community, ministries of interior, defence, transportation, and foreign affairs; law enforcement; customs and coast guard and other agencies with security related responsibilities.

States will need to ensure that the regulatory body is adequately resourced, in terms of personnel and funding, to fulfil its regulatory functions, including implementing an inspection programme to verify that the security of radioactive sources is effectively maintained. This inspection programme should be supported by written procedures and performed by qualified personnel. The frequency of inspections should take account of the security level (see Section 4.1) of the radioactive source(s) and may consider an operator's past performance in maintaining compliance with security requirements. Inspections of security measures implemented by an operator can be performed together with inspections for verifying compliance with other regulatory requirements, such as safety, or as stand-alone inspections.

2.3. OPERATORS

Operators, as the authorized entities, should have the primary responsibility for implementing and maintaining security measures for radioactive sources in accordance with national requirements. Operators may, depending on a State's regulatory requirements, appoint or contract a third party to carry out actions and tasks related to the security of radioactive sources, although the authorized operator should retain the prime responsibility for regulatory compliance and effectiveness of the actions and tasks. Also, operators should ensure that their personnel and their contractors are suitably trained and meet the regulatory requirements, which should include trustworthiness.

Operators should verify that sources are present at their authorized location at prescribed intervals. Any absence or discrepancy should be promptly investigated and reported to the regulatory body. Processes should be in place to ensure that all Category 1, 2, and 3 sources (see Section 4.2.1) for which operators are authorized are identifiable and traceable.

When required by the regulatory authorities, operators should carry out vulnerability assessments (see the Definitions) of their radioactive sources based on the current assessed threat.

Operators should promote a security culture (see Section 3.2), and establish a management system commensurate with the levels of security (see Section 4.1), to ensure that:

— Policies and procedures are established that identify security as being of high priority;
— Problems affecting security are promptly identified and corrected in a manner commensurate with their importance;
— The responsibilities of each individual for security are clearly identified and each individual is suitably trained, qualified, and determined to be trustworthy;
— Clear lines of authority for decisions on security are defined;
— Organizational arrangements and lines of communications are established that result in an appropriate flow of information on security within the entire organization;
— Sensitive information is identified and protected according to national regulations;
— Radioactive sources are managed in accordance with a security plan (see the Definitions), when required by the regulatory body.

3. SECURITY CONCEPTS

3.1. INTRODUCTION

This section introduces the basic principles applicable to the security of radioactive sources established in the Code of Conduct [1], and then elaborates on security concepts, including the basic security functions of deterrence, detection, delay, response and security management (Table 1).

3.2. SECURITY CULTURE

A dynamic and effective security culture should exist at all levels of operator staff and management.

TABLE 1. PRINCIPLES FROM THE CODE OF CONDUCT FOR THE SECURITY OF RADIOACTIVE SOURCES

The Code of Conduct establishes basic principles applicable to the security of radioactive sources, several of which are relevant to this publication. According to these principles, every State has:

- To take the appropriate measures necessary to ensure that radioactive sources are **"securely protected during their useful lives and at the end of their useful lives"** (paragraph 7);
- To emphasize "to designers, manufacturers (both manufacturers of radioactive sources and manufacturers of devices in which radioactive sources are incorporated), suppliers and users and those managing disused sources **their responsibilities for the safety and security of radioactive sources**" (paragraph 15);
- To define "its **domestic threat**, and **assess its vulnerability** with respect to this threat for the variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources" (paragraph 16);
- To have legislation and regulations in place for "requirements for **security measures to deter, detect, and delay** the unauthorized access to, or the theft, loss or unauthorized use or removal of radioactive sources during all stages of management" (paragraph 19);
- To ensure that "the regulatory body established by its legislation has the authority to attach clear and unambiguous conditions to the authorizations issued by it, including conditions relating to:…(viii) measures to determine, as appropriate, the **trustworthiness** of individuals involved in the management of radioactive sources; and (ix) the **confidentiality of information** relating to the security of sources" (paragraph 20);
- To ensure that its regulatory body has the authority to **require a security plan or assessment, as appropriate, and to promote the establishment of a security culture** among all individuals and in all bodies involved in the management of radioactive sources (paragraphs 20 and 22).

The characteristics of security culture are the beliefs, attitudes, behaviour and management systems, the proper assembly of which lead to more effective security.

The foundation of security culture is a recognition — by those that have a role in regulating, managing or operating facilities or activities involving radioactive sources, or even those that could be affected by these activities — that a credible threat exists and that security is important.

Readers of this guide should also read Nuclear Security Culture [14], which describes the basic concepts and elements of security culture.

Security culture may be enhanced by various means including, as appropriate:

— Assigning responsibility for the security of radioactive sources to a senior staff member, but ensuring that staff members are aware that security is a shared responsibility across the whole organization;
— Documenting legal and regulatory security responsibilities applying to the operator and bringing this to the attention of relevant managers, staff and, where appropriate, all employees and contractors;
— Ensuring threat awareness and training security managers, response personnel and all personnel with secondary responsibilities for security;
— Addressing security matters in staff and contractor induction courses;
— Providing security instructions and ongoing security awareness briefings to staff and contractors, and training and evaluation of the lessons learned;
— Conducting regular performance testing and preventive maintenance.

3.3. PURPOSE OF A SECURITY SYSTEM

A security system should be designed by the operator's security professionals to deter adversaries from committing a malicious act or to minimize through detection, delay and response the likelihood of an adversary succeeding in completing such a malicious act. Such an act would consist of a sequence of actions by one or more adversaries (threat) to obtain access to a source (target) either in order to commit an act of sabotage or another malicious act, or in order to remove the source without authorization.

3.4. SECURITY FUNCTIONS

A security system to protect radioactive sources from an adversary intent on committing a malicious act should be designed to perform basic security functions: deterrence, detection, delay, response, and security management:

— ***Deterrence*** occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt. Deterrent measures have the effect of convincing the adversary that the malicious act would be too difficult, the success of the act too uncertain, or the consequence of the act to the adversary too unpleasant to justify the undertaking. Measures designed specifically to deter thus involve communication to the adversary about the presence of measures

performing the other security functions. If this communication has the intended effect, deterrence is the result.

— ***Detection*** is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of a radioactive source. Detection can be achieved by several means, including visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems, and other means. Adversary awareness of detection measures can also serve as a deterrent.

— ***Delay*** impedes an adversary's attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means. A measure of delay is the factor of time, after detection, that is required by an adversary to remove or sabotage the radioactive source. Adversary awareness of delay barriers can also serve as a deterrent.

— ***Response*** encompasses the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. These actions, typically performed by security or law enforcement personnel, and other State agencies, include interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using the radioactive source to cause harmful consequences, recovering the radioactive source, or otherwise reducing the severity of the consequences. The prospect of successful response can also serve as a deterrent.

— ***Security management*** includes ensuring adequate resources (personnel and funding) for the security of sources. It also includes developing procedures, policies, records, and plans for the security of sources and for a more effective security culture, in general. This term also includes developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure.

3.5. DESIGN AND EVALUATION OF SECURITY SYSTEMS

A well designed security system should integrate measures to perform all five security functions so as to effectively secure the target from the threat, consistent with the following security concepts:

Deterrence cannot be measured: The objective of deterrence is to dissuade an adversary from attempting a malicious act. As a result, the impact of deterrent measures cannot be quantified. Therefore, the design of a security system should not be wholly based on deterrence.

Detection before delay: The function of delay is to provide response personnel with sufficient time to deploy and interrupt or interdict the adversary's efforts to complete a malicious act. Therefore, detection must precede delay. If an adversary is given the opportunity to overcome barriers and other obstacles prior to encountering intrusion sensors or other detection means, the adversary will have completed the most difficult tasks before being detected and thus may well succeed in removing or sabotaging the radioactive source before the response personnel arrive. In this case, barriers do not serve as a delay but rather, at most, as deterrents.

Detection requires assessment: Most means of detection provide an indirect indication of potential malicious action, such as attempted unauthorized access, removal or sabotage of a radioactive source. The only direct indication is by direct human observation. Therefore, when an alarm, or other indirect indication is triggered, there is always some uncertainty as to the cause. As a result, detection should always be complemented by assessment to determine the cause of the alarm. Alarm assessment requires human observation and judgment, through deployment of response personnel to investigate the cause of the alarm, through remote closed circuit television (CCTV) systems, or similar means. Sometimes, adversaries may attempt to exploit any delay between detection and assessment to mask their malicious intent. Therefore, immediate assessment is the goal of any security system.

Delay greater than assessment plus response time: A security system is successful if it detects and a correct assessment is made of an adversary attempting a malicious act in sufficient time for subsequent delay measures to permit response personnel to interrupt and stop the adversary prior to completion of the act or to initiate prompt actions to mitigate potentially high consequences. This relationship of the functions of detection, delay and response is known as *timely detection.*

Balanced protection: This is a concept of equivalent security functions (deterrence, detection delay, response, and security management) that provides adequate protection against all threats along all possible pathways. In other words, delay times through each pathway, detection measures associated with each detection element and the resulting responses provide the necessary protection to prevent a successful act.

Defence in depth: A concept of several layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve their objective.

3.6. INTEGRATION OF SAFETY AND SECURITY MEASURES

Safety measures and security measures have in common the aim of protecting human life and health and the environment. Safety measures and security measures should be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security. In implementing the recommendations in this guide, the designers of security systems should consult with qualified safety experts to ensure that security measures do not compromise the safety of individuals or the protection of the environment.

3.7. GRADED APPROACH TO SECURITY

Security requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness of a radioactive source, the nature of the source and potential consequences associated with its unauthorized removal or sabotage. This graded approach ensures that the highest consequence sources receive the greatest degree of security.

3.8. UNDERSTANDING AND ADDRESSING THE THREAT ENVIRONMENT

The design and evaluation of a security system should take into account the current national threat assessment and may include the development and application of a design basis threat (DBT) (see the Definitions).

3.8.1. National threat assessment

The Code of Conduct states:

> "Every State should define its domestic threat, and assess its vulnerability with respect to this threat for the variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources."

The procedure for meeting this principle should begin with a national threat assessment, which is an analysis that documents at a national level the credible motivations, intentions, and capabilities of potential adversaries that

could cause harm through the sabotage of a facility or the unauthorized removal of a radioactive source for malicious purposes. Typically, such an assessment is conducted by a State's intelligence community, often with input from such agencies as ministries of interior, defence, transportation, and foreign affairs; law enforcement; customs and coast guard; and other agencies with security related responsibilities, and may include the regulatory body. If not previously involved in this assessment, the regulatory body should be informed of the threat as currently assessed by the relevant national agencies for use in the development of its regulatory programme for security of radioactive sources.

The assessment process is one of deductive reasoning. Starting from what is known, a judgment is made about how adversary groups or individuals may behave in the future. This would include, for example, historic events and known capabilities to attack the types of facilities where radioactive sources are stored or used. The threat assessment should cover at least the following attributes and characteristics for each identified insider and external adversary:

— *Motivation*. Political, financial, ideological, personal.
— *Level of commitment*. Disregard for personal health, safety, well-being, or survival.
— *Intentions.* Material or facility sabotage (unauthorized removal), public panic and disruption, political instability, mass injuries and casualties.
— *Group size.* Attack force, coordination, support.
— *Weapons.* Types, numbers, availability, improvised.
— *Tools.* Mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment.
— *Modes of transport*. Public, private, land, sea, air, type, number, availability.
— *Technical skills.* Engineering, use of explosives and chemicals, paramilitary experience, communication skills.
— *Cyber skills.* Using computers and automated control systems in direct support of physical attacks, for intelligence gathering, for computer based attacks, for money collection, etc.
— *Knowledge.* Targets, site plans and procedures, security measures, safety and radiation protection procedures, operations, potential use of nuclear or other radioactive material.
— *Funding*. Source, amount, availability.
— *Insider issues.* Collusion, passive/active, violent/non-violent, number of insiders.
— *Support structure.* Local sympathizers, support organization, logistics;
— *Tactics.* Covert and overt.

Once the State has made an assessment of its threat, it will need to decide on a basis for establishing its regulations for the security of radioactive sources. One approach is to establish regulations on the basis of the national threat assessment while another is to regulate on the basis of the DBT (see below), for which the national threat assessment becomes an input. In selecting a regulatory basis, there are several factors that need to be considered by the State, including the severity of consequences associated with malicious acts involving radioactive sources in the State, determination by the State of the ability to establish effective protection systems using each approach, and the ability of the regulatory body to implement the different approaches.

It is worth noting that all States need not use a DBT approach for their regulatory system. However, if a DBT approach is not selected, the State will still need to prepare a national threat assessment and keep it current.

3.8.2. Design basis threat

A DBT, defined at the State level, is a tool used to help establish performance requirements for the design of physical protection systems for specific types of facilities. It is also used to help operators and State authorities assess the effectiveness of the systems to counter adversaries by evaluating the systems' performance against adversary capabilities described in the DBT, by conducting vulnerability assessments. A DBT is a comprehensive description of the motivations, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. The capabilities of the adversary, whether an insider or external, help determine the detection, delay, and response requirements for a physical protection system to be effective against a DBT.

The development of a DBT will be specific to each State, due to social, cultural and geopolitical differences. As with the national threat assessment, developing a DBT typically requires the combined efforts of domestic authorities such as intelligence and security agencies, law enforcement and regulatory bodies and operators. The DBT may need to be reviewed from time to time in the light of new information from State organizations. More detailed information on the DBT process can be found in Ref. [13].

3.8.3. Insider threats

Insider threats should be given particular attention when designing a security system. Such threats could stem from one or more persons with legitimate access to a facility and detailed knowledge of activities or source locations. These individuals may be employees or contractors who could

remove radioactive sources or information, with malicious intent, or conduct acts of sabotage on the premises. Moreover, individuals may seek employment at a facility with the intention of committing malicious acts and may also assist external adversaries to remove sources or carry out hostile acts. Insider threats and recommended appropriate countermeasures are further explained in Ref. [15].

3.8.4. Increased threat

A security system should be effective in countering the currently assessed threat. However, there should be provisions to ensure that the security status can be temporarily heightened during times of increased threat. This should include the introduction of additional security measures or reduction in the accessibility to the radioactive sources.

3.9. VULNERABILITY ASSESSMENT

A vulnerability assessment (VA), also known as a security survey or security assessment, is a method for evaluating protective security systems. It is a systematic appraisal of the effectiveness of a security system for protection against an assessed threat (or DBT if one exists). The VA can be specific or general in nature, can be conducted locally by the operator or by the State/regulatory body, and can be used to help the development of regulations by the State/regulatory body or for demonstrating regulatory compliance of the operator. Additional information on how to perform a VA can be found in Appendix III.

4. ESTABLISHING A REGULATORY PROGRAMME FOR RADIOACTIVE SOURCE SECURITY

The provisions in the Code of Conduct relating to the security of radioactive sources have been strengthened to provide measures to reduce the likelihood of malicious acts. The Code also specifically mentions that States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes. In case of such an event, requirements and guidance on

emergency preparedness and response, intervention and the remediation of contaminated areas are available from the IAEA [5, 9, 10]. Guidance on protecting people against radiation in the aftermath of a radiological attack is given by the International Commission on Radiological Protection [11].

Such malicious acts and potential consequences could include:

— The deliberate placement of a breached or unshielded source in a public area;
— The deliberate dispersion of radioactive material to cause adverse health effects (by using, for example, a radioactive dispersal device (RDD));
— The use of an RDD for the purposes of contaminating ground, buildings and infrastructure leading to denial of access to these areas, which may be based on radiation protection criteria, economic impact and the cost of clean up and reconstruction.

Many States already have a regulatory programme in place that covers activities such as authorization, review and assessment, inspection and enforcement [16]. This section provides guidance to regulatory bodies on how to develop or enhance regulatory programmes to address the security of radioactive sources in order to reduce the likelihood of malicious acts involving those sources. Safety and security measures should be designed and implemented in an integrated manner so that they do not compromise each other.

Establishing such a regulatory programme for the security of radioactive sources involves three basic steps for the regulatory body:

— **Step 1:** Establish graded security levels with corresponding goals and objectives for each security level (see Section 4.1).

— **Step 2:** Determine the security level applicable to a given source (see Section 4.2).

— **Step 3:** Select and implement a regulatory approach (prescriptive, performance based, or combined) for directing operators as to how to design, implement and evaluate security measures in order to meet the security objectives in Table 1 (see Section 4.3).

4.1. STEP 1: ESTABLISH GRADED SECURITY LEVELS WITH CORRESPONDING GOALS AND OBJECTIVES

Radioactive sources have a wide range of characteristics (such as activity) that make them attractive in varying degrees to adversaries. A corresponding range of effective security measures should be utilized to ensure that the sources are adequately protected using a graded approach. In order to ensure adequate security capability without imposing overly restrictive measures, the concept of security levels should be used. Three security levels (A, B, and C) have been developed to allow specification of security system performance in a graded manner. Security level A requires the highest degree of security while the other levels are progressively lower.

Each security level has a corresponding goal. The goal defines the overall result that the security system should be capable of providing for a given security level. The following goals have been developed:

— **Security level A**: *Prevent* unauthorized removal of a source.
— **Security level B**: *Minimize the likelihood* of unauthorized removal of a source.
— **Security level C**: *Reduce the likelihood* of unauthorized removal of a source.

Malicious acts can involve either unauthorized removal of a source or sabotage. While the security goals only address unauthorized removal, achievement of the goals will reduce the likelihood of a successful act of sabotage. Security systems that achieve the goals listed above will provide some (although limited) capability to detect and respond to an act of sabotage.

In order to meet the *goals*, it is necessary to achieve an adequate level of performance for each of the security *functions*: deterrence, detection, delay, response, and security management. That level of performance is defined as a set of *objectives* for each of the functions. These objectives state the desired outcome from the combination of *measures* applied for that objective. Deterrence is a security function which is difficult to quantify. Consequently, it has not been assigned an associated set of security objectives and measures in this publication.

Security levels and associated security objectives are summarized in Table 2.

Where an objective is shown in Table 2 as the same for two or more security levels, it is intended that the objective be met in a more rigorous manner for the higher security level.

TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES

Security functions	Security objectives		
	Security Level A Goal: Prevent unauthorized removal[a]	Security Level B Goal: Minimize likelihood of unauthorized removal[a]	Security Level C Goal: Reduce likelihood of unauthorized removal[a]
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions)		
	Establish security event reporting system		

[a] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

4.2. STEP 2: DETERMINE THE SECURITY LEVEL APPLICABLE TO A GIVEN SOURCE

In order to specify an appropriate security level for a source, consideration should be given to the potential harm that the source could cause if it were used in a malicious act. This potential for harm then guides the process of assigning an appropriate security level to the source. This process consists of the following steps:

— Categorizing sources based on the potential to cause harm if used for malicious purposes (including aggregation of sources in a given location as appropriate) (see Section 4.2.1);
— Assigning an appropriate security level to each category (see Section 4.2.2).

4.2.1. Categorization of radioactive sources

The Code of Conduct applies to radioactive sources that may pose a significant risk to individuals, society, and the environment, i.e. sources in Categories 1–3. Appropriate security measures should be applied to reduce the likelihood of malicious acts involving these sources.

The source categorization used in the Code of Conduct is based on the concept of 'dangerous sources' which are quantified in terms of D values [17]. This concept is further discussed in the IAEA's Categorization of Radioactive Sources [3]. This publication provides a recommended system of categorization, particularly for those sources used in industry, medicine, agriculture, research and education. This system of categorization can also be applied, where appropriate, in the national context, to sources within military or defence programmes. The categorization provides an internationally harmonized basis for risk informed decision making and is based on a logical and transparent method that provides the flexibility for it to be applied in a wide range of circumstances. The risk informed decisions can be made in a graded approach to the regulatory control of radioactive sources for the purposes of safety and security.

In recognition of the fact that human health is of paramount importance, the categorization system is based primarily on the potential for radioactive sources to cause deterministic health effects. The D value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects for a range of scenarios that include both external exposure from an unshielded source and inadvertent internal exposure following dispersal (e.g. by fire or explosion) of the source.

The activity of the radioactive material (A) in sources varies over many orders of magnitude; D values are therefore used to normalize the range of activities in order to provide a reference in comparing risks. This should be done by taking the activity A of the source (in TBq) and dividing it by the D value for the relevant radionuclide.

It should be noted that there is the potential for amounts of material less than the D values to be dangerous [17]. This could be the case in the event of malicious administration of unsealed radioactive material to an individual.

The activity thresholds for radionuclides in the Code of Conduct for source Categories 1–3 are listed in Table 3. For radionuclides not found in this table, please see Refs. [3, 17].

In some situations it may be appropriate to categorize a source on the basis of A/D alone, e.g. when intended use of the source is unknown or not confirmed. However, when the circumstances of use of the source are known, the regulatory body may make a judgment to modify this initial categorization using other information about the source or its use. In some circumstances it may be convenient to assign a category on the basis of the intended use of the source (see Table 4).

The categorization system has five categories, as shown in Table 4. This number of categories should be sufficient to enable the practical applications of the scheme, without unwarranted precision. Within this categorization system, sources in Category 1 are considered to be the most 'dangerous' because they can pose a very high risk to human health if not managed safely and securely. An exposure of only a few minutes to an unshielded Category 1 may be fatal. At the lower end of the categorization system, sources in Category 5 are the least dangerous; however, even these sources could give rise to doses in excess of the dose limits if not properly controlled, and therefore should be kept under appropriate regulatory control. Categories should not be subdivided as this would imply a degree of precision that is not warranted and could lead to a loss of international harmonization.

4.2.1.1. Unlisted sources

For radioactive sources not listed in Table 4, the regulatory body may assign a category to the source based on the A/D ratio.

4.2.1.2. Short half-life radionuclides

In some activities, such as nuclear medicine, radionuclides with a short half-life are used in a source form that is unsealed. Examples of such

TABLE 3. ACTIVITIES CORRESPONDING TO THRESHOLDS OF CATEGORIES

Radionuclide	Category 1 1000 ×D		Category 2 10 ×D		Category 3 D	
	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]	(TBq)	(Ci)[a]
Am-241	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Am-241/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Cf-252	2.E+01	5.E+02	2.E-01	5.E-00	2.E-02	5.E-01
Cm-244	5.E+01	1.E+03	5.E-01	1.E+01	5.E-02	1.E+00
Co-60	3.E+01	8.E+02	3.E-01	8.E+00	3.E-02	8.E-01
Cs-137	1.E+02	3.E+03	1.E+00	3.E+01	1.E-01	3.E+00
Gd-153	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Ir-192	8.E+01	2.E+03	8.E-01	2.E+01	8.E-02	2.E+00
Pm-147	4.E+04	1.E+06	4.E+02	1.E+04	4.E+01	1.E+03
Pu-238	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Pu-239[b]/Be	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ra-226	4.E+01	1.E+03	4.E-01	1.E+01	4.E-02	1.E+00
Se-75	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Sr-90 (Y-90)	1.E+03	3.E+04	1.E+01	3.E+02	1.E+00	3.E+01
Tm-170	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Yb-169	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Au-198*	2.E+02	5.E+03	2.E+00	5.E+01	2.E-01	5.E+00
Cd-109*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02
Co-57*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Fe-55*	8.E+05	2.E+07	8.E+03	2.E+05	8.E+02	2.E+04
Ge-68*	7.E+02	2.E+04	7.E+00	2.E+02	7.E-01	2.E+01
Ni-63*	6.E+04	2.E+06	6.E+02	2.E+04	6.E+01	2.E+03
Pd-103*	9.E+04	2.E+06	9.E+02	2.E+04	9.E+01	2.E+03
Po-210*	6.E+01	2.E+03	6.E-01	2.E+01	6.E-02	2.E+00
Ru-106 (Rh-106)*	3.E+02	8.E+03	3.E+00	8.E+01	3.E-01	8.E+00
Tl-204*	2.E+04	5.E+05	2.E+02	5.E+03	2.E+01	5.E+02

[a] The primary values to be used are given in TBq. Curie values are provided for practical usefulness and are rounded after conversion.

[b] Criticality and safeguards issues will need to be considered for multiples of D.

* These radionuclides are very unlikely to be used in individual radioactive sources with activity levels that would place them within Categories 1, 2 or 3 and would, therefore, not be subject to those paragraphs of the Code relating to national registries or to import and export controls.

TABLE 4. CATEGORIES FOR COMMONLY USED SOURCES

Category	Source[a]	A/D[b]
1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	$A/D \geq 1000$
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	$1000 > A/D \geq 10$
3	Fixed industrial gauges that incorporate high activity sources[c] Well logging gauges	$10 > A/D \geq 1$
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	$1 > A/D \geq 0.01$
5	Low dose rate brachytherapy eye plaques and permanent implant sources X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt[d]

[a] Factors other than A/D alone have been taken into consideration in assigning the sources to a category (see Ref. [3], Annex I).

[b] This column can be used to determine the category of a source purely on the basis of A/D. This may be appropriate, for example, if the facilities and activities are not known or are not listed, if sources have a short half-life and/or are unsealed, or if sources are aggregated (see Ref. [3], paragraph 3.5).

[c] Examples are given in Ref. [3], Annex I.

[d] Exempt quantities are given in Schedule I of Ref. [5].

applications include ^{99m}Tc in radiodiagnosis and ^{131}I in radiotherapy. In such situations, the principles of the categorization system may be applied to determine a category for the source. These situations should be considered on a case by case basis.

4.2.1.3. Unsealed radioactive sources

The regulatory body may assign a category to unsealed radioactive sources based on the A/D ratio.

4.2.1.4. Radioactive decay

If the activity of a source decays to a level below the appropriate threshold in Table 3 or below that which is normally used (as shown in Table 4), the regulatory body may allow the operator to recategorize the source based on the A/D ratio.

4.2.1.5. Aggregation of sources

There will be situations in which radioactive sources are in close proximity, such as in manufacturing processes (e.g. in the same room or building) or in storage facilities (e.g. in the same enclosure). In such circumstances, the regulatory body may wish to aggregate the activity in the sources to determine a situation specific categorization for the purposes of implementing regulatory control measures. In situations of this type, the summed activity of the radionuclide should be divided by the appropriate D value and the calculated ratio A/D compared with the ratios of A/D given in Table 2, thus allowing the set of sources to be categorized on the basis of activity. If sources with various radionuclides are aggregated, then the sum of the ratios A/D should be used in determining the category, in accordance with the formula:

$$\text{Aggregate A/D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

where:

$A_{i,n}$ = activity of each individual source i of radionuclide n.
D_n = D value for radionuclide n.

Additional information on the aggregation of radioactive sources may be found in Ref. [3].

4.2.2. Assigning security levels

As a default arrangement, the regulatory body could use the categories listed above to assign the security level applicable to a given source.

Category 1 sources should have security measures which meet the security objectives of Security Level A. Category 2 sources should have security measures which meet the security objectives of Security Level B. Category 3 sources should have security measures which meet the security objectives of Security Level C.

The International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (paragraph 2.34 [5]) include general requirements for the security of radioactive sources. This guide considers that while those control measures provide a sufficient level of security for radioactive sources in Categories 4 and 5, enhanced measures specified in this guide should be applied to radioactive sources in Categories 1, 2 and 3 in order to reduce the likelihood of malicious acts involving those sources. Furthermore, the regulatory body, taking account of its national threat, may wish to enhance the security of sources in Categories 4 and 5 sources in appropriate circumstances. This approach is summarized in Table 5.

While this approach can be viewed as a default position, the malicious use of radioactive sources may not necessarily involve sources that are ranked highest in this categorization scheme. Most Category 1 sources, for example, will be held within shielding and inside fixed devices or facilities. Efforts to remove the source would take time and may expose the adversaries to a significantly harmful level of radiation. It is, therefore, possible that adversaries will focus on sources of a lower category, more accessible, less of a hazard to handle, portable, and more easily concealed.

The purpose of categorizing radioactive sources is to provide an internationally accepted basis for risk informed decision making, including measures to reduce the likelihood of malicious acts. However, socioeconomic consequences resulting from malicious acts were excluded from the categorization criteria as no methodology for quantifying and comparing these consequences exists, especially on an international basis.

4.2.3. Additional considerations for assigning security levels

Annex I of the Code of Conduct notes that States should give appropriate attention to radioactive sources considered by them to have the potential to cause unacceptable consequences if employed for malicious purposes.

Although Refs [3, 17] already take into account some of the factors below, the regulatory body needs to pay special attention to these factors and

TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES

Category	Source	A/D	Security level
1	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D ≥ 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D ≥ 10	B
3	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D ≥ 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D ≥ 0.01	Apply measures as described in the Basic Safety Standards [5]
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

considerations when assigning security levels to radioactive sources. These factors represent variables that are specific to the source and the manner and location in which it is used — and these may affect the level of security that is appropriate for a given source or facility.

4.2.3.1. Attractiveness of sources

In addition to the activity of a source, there are other factors that may make some sources more attractive for use in malicious acts. These factors include:

— The chemical and physical form of the radioactive material in the source, which may make it easily dispersible and hence more attractive to an adversary.
— The nature of the radioactive emission. Some radionuclides produce higher doses per unit intake than others, notably alpha emitters. Sources containing these radionuclides may be more attractive for use in an RDD.
— Ease of handling. Sources that can be easily handled or are easily accessible may be more attractive since the adversary will be less likely to receive a high radiation dose and the source is more easily moved. An example of this is a source inside a self-shielded portable device.
— Co-location. Multiple sources or large quantities of radioactive material that are co-located may be attractive to an adversary since successful penetration of the security system may allow removal or sabotage of sufficient material to produce very serious consequences.
— Perceived economic value of the source or the equipment it may be inside.

The regulatory body may wish to consider the attractiveness of sources in determining the security level assigned to a source and the security measures applied to that security level.

4.2.3.2. Sources in storage

Radioactive sources placed in storage should be protected in accordance with the measures reflected in this publication and according to the categorization and security level applied to the source.

4.2.3.3. Vulnerability and threat level

The domestic threat level and any increases in it may warrant evaluation of the security level assigned to a source, taking into account all other attributes of the source (e.g. attractiveness, vulnerability). Alternatively, specific security measures for a given security level may also be strengthened.

4.2.3.4. Mobile, portable and remote sources

Sources used in field applications (e.g. radiography and well logging) are typically contained in devices designed for portability and are frequently transported between job sites. The ease of handling of these devices and their presence in vehicles outside secured facilities make them attractive for unauthorized removal.

Recognizing that security measures for fixed sources may not be practical for application to sources used in the field, alternative measures should be applied to achieve the security objective. Please refer to the detection and delay measures for Security Levels B and C (Section 4.3.1), as well as the illustrative security measures for mobile sources in Appendix IV.

Sources that are used in remote locations could be removed by unauthorized personnel and transported out of the area before effective response is possible.

The regulatory body may wish to consider mobility, portability and location when assigning a security level to a source or may wish to consider additional measures within the assigned security level to compensate for these conditions.

4.3. STEP 3: SELECT AND IMPLEMENT A REGULATORY APPROACH

There are three alternative approaches that the regulatory body may use for directing operators on how to demonstrate that they meet the security objectives specified in Table 2. The approach(es) selected by the regulatory body should take into account its own capabilities and resources, the capabilities and resources of the operators that it regulates, and the range of sources that should be protected:

— A *prescriptive approach* establishes specific security measures determined by the regulatory body to meet the security objectives for each security level. The guidance in this section identifies a set of such measures for each security level, which the regulatory body may adopt as requirements in the absence of a DBT. Alternatively, the regulatory body may use the security measures in this guidance as a starting point, but tailor them to national circumstances. Use of the prescriptive approach is particularly appropriate in cases where the combination of threat and potential consequences is low or where conducting a detailed threat assessment is not possible. The prescriptive approach has the advantage

of simplicity in implementation for both the regulatory body and operators, and also ease of inspection and auditing. The disadvantage of this approach is its relative lack of flexibility to address actual circumstances. For example, experience has shown that an operator can be in compliance with prescribed measures, and yet not meet the aim of the security system to protect the targets from the actual or defined threat. Consequently, when the prescriptive approach is used, the regulatory body needs to ensure that inspections or security assessments are performed to evaluate the overall effectiveness of the facility's security system in meeting the security goal and objectives for the applicable security level (see Section 4.3.1).

— A *performance based approach* is one where the regulatory body allows flexibility for the operator to propose the particular combination of security measures that will be used to achieve the security objectives in Table 2. The proposed security measures should be based on vulnerability assessment, taking into account information provided by the regulatory body, based on a national threat assessment and, where applicable, a DBT. The advantages of this approach are that it recognizes that an effective security system can be composed of many combinations of security measures, and that each operator's circumstances can be unique. The prerequisite for this approach is that it requires both the operator and the regulatory body to have relatively high levels of security expertise (see Section 4.3.2).

— A *combined approach* includes elements drawn from both prescriptive and performance based approaches. There are many possible versions of the combined approach. For example, the regulatory body may adopt a set of security measures from which the operator may choose, while requiring the operator to demonstrate that the security system as a whole meets the applicable security objectives. Alternatively, the regulatory body could use a performance-based approach for the radioactive sources with the highest potential consequences of malicious use and a prescriptive approach for lower consequence sources. Or, a set of prescriptive requirements could be supplemented with performance-oriented requirements addressing particular matters. The main advantage of the combined approach is the flexibility it allows (see Section 4.3.3).

The remainder of this section provides guidance to regulatory bodies for using each approach.

4.3.1. Prescriptive approach

The regulatory body may choose to specify security measures that operators are required to have in place in order to meet the security objectives in Table 2. Tables 6, 7 and 8 specify security measures intended to meet the security objectives of Security Levels A, B and C, respectively. These tables include security measures for sources in use or in storage. The measures are discussed in detail after each corresponding table. The measures may vary depending on whether a given source is in use or in storage, or is a mobile or portable source. More information on some of these measures can be found in Appendix I. Illustrative security measures that may be applied to selected facilities and activities are provided in Appendix IV.

Introduction for Security Level A measures

The goal of Security Level A is to **prevent the unauthorized removal** of radioactive sources. If an attempt at unauthorized access or unauthorized removal were to occur, detection and assessment have to occur early enough to enable response personnel to respond with enough time and with sufficient resources to interrupt the adversary and prevent the source from being removed. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection system and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see the section on 'Delay' below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of immediate intrusion detection.

TABLE 6. RECOMMENDED MEASURES FOR SECURITY LEVEL A
(goal: prevent unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location.	Electronic intrusion detection system and/or continuous surveillance by operator personnel.
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider.	Electronic tamper detection equipment and/or continuous surveillance by operator personnel.
	Provide immediate assessment of detection.	Remote monitoring of CCTV or assessment by operator / response personnel.
	Provide immediate communication to response personnel.	Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.
	Provide a means to detect loss through verification.	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.	Capability for immediate response with size, equipment, and training to interdict.
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
	Ensure trustworthiness of authorized individuals.	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security-related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

Security objective: Provide immediate detection of any attempted unauthorized removal of the source (e.g. an insider).

Security measures: Electronic tamper detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. For mobile sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal. Note, however, that if continuous surveillance is chosen as a security measure, continuous visual surveillance may require observation by at least *two* individuals at all times to protect against an insider scenario.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/ response personnel.

Once an intrusion detection or tamper detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with diverse (at least two) means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Daily checking through physical checks, CCTV, tamper indicating devices, etc.

Daily checking should consist of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, remote observation through CCTV, verification of seals or other tamper evident devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.

Security measures: System of least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict.

A balanced system comprising at least two barriers should separate the source from unauthorized personnel and provide sufficient delay following detection to enable response personnel to intercede before the adversary can remove the source. For sources in use, such measures may include a locked device in a secured area to separate the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source in a locked storage room, thus separating the container from unauthorized personnel. For mobile sources in use, continuous visual surveillance by operator personnel may substitute for one or both layers of barriers.

Response

Security objective: Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.

Security measures: Capability for immediate response with size, equipment, and training to interdict.

The operator should establish protocols to ensure immediate deployment of response personnel without delay in response to an alarm. The response should be both immediate and adequate. *Immediate* means that responders should arrive, once notified, in a time shorter than the time required to breach the barriers and perform the tasks needed to remove the source. *Adequate* means that the response team is of sufficient size and capability to subdue the adversary. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as a locked door (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure, patients do not need to be 'authorized' since they are escorted to the source and are under constant surveillance by the medical staff.)

The identity and authorization of a person seeking access can be verified by such measures as:

— Personal identification number (PIN) to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system allows that person to enter the secured area or source location, e.g. by opening a lock. A combination of two or more verification measures should be required, e.g. the use of a swipe card and a PIN; or the use of a swipe card and a controlled key; or a PIN and a computer password; or the use of a controlled key and visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile sources in use, continuous

visual surveillance by multiple operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security of radioactive sources, it is necessary to protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

— The specific location and inventory of sources;
— The relevant security plan and detailed security arrangements;
— Security systems (e.g. intruder alarms) including performance and installation diagrams;
— Temporary or longer term weaknesses in the security programme;
— Security staffing arrangements and the means of response to events or alarms;
— Planned dates, routes and mode of shipment or transfer of sources;
— Contingency plans and security response measures.

Regulatory guidance should also provide for:

— Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
— Recommended methods for the destruction of documents containing sensitive information;
— Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be authorized by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored between periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans

Security measures: Procedures for responding to security-related scenarios

At each facility security contingency plans should be drawn up for a range of events, including:

— A suspected or threatened malicious act;
— A public demonstration which has the potential to threaten the security of sources;
— An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Security contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting of security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;
— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— The discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
— Failure or loss of security systems that are essential to the protection of radioactive sources.

TABLE 7. RECOMMENDED MEASURES FOR SECURITY LEVEL B
(goal: minimize the likelihood of unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion detection equipment and/or continuous surveillance by operator personnel
	Provide detection of any attempted unauthorized removal of the source	Tamper detection equipment and/or periodic checks by operator personnel

TABLE 7. RECOMMENDED MEASURES FOR SECURITY LEVEL B
(goal: minimize the likelihood of unauthorized removal) (cont.)

Security function	Security objective	Security measures
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator / response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phones, cell phones, pagers, radios
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper detection equipment, etc.
Delay	Provide delay to minimize the likelihood of unauthorized removal	System of two layers of barriers (e.g. walls, cages)
Response	Provide immediate initiation of response to interrupt unauthorized removal	Equipment and procedures to immediately initiate response
Security management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measure
	Ensure trustworthiness of authorized individuals	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security event reporting system	Procedures for timely reporting of security events

Introduction for Security Level B measures

The goal of Security Level B is to **minimize the likelihood of unauthorized removal** of radioactive sources. If an attempt of unauthorized access or unauthorized removal were to occur, the response must be initiated immediately upon detection and assessment of the intrusion, but the response is not required to arrive in time to prevent the source from being removed. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see section on 'Delay' below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of intrusion detection.

Security objective: Provide detection of any attempted unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Tamper detection equipment or visual surveillance by operator personnel made during periodic checks indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. This may be facilitated by the use of electronic tamper detection equipment. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/ response personnel.

Once an intrusion detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable means of communication such as phones, cell phones, pagers, radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with dependable means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Weekly checking through physical checks, tamper detection equipment, etc.

Weekly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper evident devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to minimize the likelihood of unauthorized removal.

Security measures: System of two layers of barriers (e.g. walls, cages).

A balanced system of two barriers should separate the source from unauthorized personnel. For sources in use, such measures may include a locked device in a secured area, separating the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source and a locked storage room, separating the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for barriers.

Response

Security objective: Provide immediate initiation of response to interrupt unauthorized removal.

Security measures: Equipment and procedures to immediately initiate response.

The operator should establish protocols to ensure immediate deployment of response personnel without delay, in response to an alarm, to interrupt the adversary action. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie. The response should be coordinated with local authorities to mitigate the potential consequences.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

The purpose of access control is to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as locked doors (delay measures) upon verification of the

person's identity and access authorization (in the context of medical exposure, patients do not need to be 'authorized').

The identity and authorization of a person seeking access can be verified by such measures as:

— A PIN to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's national regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security of radioactive sources, the security system should protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

— The specific location and inventory of sources;
— The relevant security plan and detailed security arrangements;
— Security systems (e.g. intruder alarms) including performance and installation diagrams;
— Temporary or longer term weaknesses in the security programme;
— Security staffing arrangements and the means of response to events or alarms;
— Planned dates, routes and mode of shipment or transfer of sources;
— Contingency plans and security response measures.

Regulatory guidance should also provide for:

— Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
— Recommended methods for the destruction of documents containing sensitive information;
— Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be approved by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored during periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and

prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

At each facility contingency plans should be drawn up for a range of events, including:

— A suspected or threatened malicious act;
— A public demonstration which has the potential to threaten the security of sources;
— An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;
— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— The discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;

— Failure or loss of security systems essential for the protection of radioactive sources.

TABLE 8. RECOMMENDED MEASURES FOR SECURITY LEVEL C
(goal: reduce the likelihood of unauthorized removal)

Security function	Security objective	Security measures
Detect	Provide detection of unauthorized removal of the source.	Tamper detection equipment and/or periodic checks by operator personnel.
	Provide immediate assessment of detection.	Assessment by operator / response personnel.
	Provide a means to detect loss through verification.	Monthly checking through physical checks, tamper indicating devices, or other checks to confirm the presence of the source.
Delay	Provide delay to reduce the likelihood of unauthorized removal of a source.	One barrier (e.g. cage, source housing) or under observation by operator personnel.
Response	Implement appropriate action in the event of unauthorized removal of a source.	Procedures for identifying necessary actions in accordance with contingency plans
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	One identification measure.
	Ensure trustworthiness of authorized individuals.	Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure.
	Provide a security plan.	Documentation of security arrangements and reference procedures.

TABLE 8. RECOMMENDED MEASURES FOR SECURITY LEVEL C
(goal: reduce the likelihood of unauthorized removal) (cont.)

Security function	Security objective	Security measures
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

Introduction for Security Level C Measures

The goal of Security Level C is to **reduce the likelihood of unauthorized removal** of radioactive sources. In order to achieve this goal, the following measures are recommended.

Detection

Security objective: Provide detection of unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Operators should verify that the sources are present. Measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Security objective: Provide immediate assessment of detection.

Security measures: Assessment by operator or response personnel.

Once tamper detection or a physical check indicates a source may be missing, there should be an immediate assessment of the situation to determine whether an unauthorized removal has actually occurred.

Security objective: Provide a means to detect loss through verification.

Security measures: Monthly checking through physical checks, tamper indicating devices, etc.

Monthly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to reduce the likelihood of unauthorized removal of a source.

Security measures: One barrier (e.g. cage, source housing) or under observation by operator personnel.

At least one physical barrier should separate the source from unauthorized personnel. For sources in use, such measures may include the source housing or use of the source in a secured area. For sources in storage, such measures may include a locked and fixed container, a device holding the source or a locked storage room to separate the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for the barrier.

Response

Security objective: Implement appropriate action in the event of unauthorized removal of a source.

Security measures: Procedures for identifying necessary actions in accordance with contingency plans.

Regulatory procedures should ensure that any suspected unauthorized removal or loss of a source is assessed and, if confirmed, reported to the appropriate authority without delay. This should be followed by an effort to locate and recover the source and investigate the circumstances leading to the event.

Security management

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to temporarily disable physical barriers such as locked doors (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure, patients do not need to be "authorized.")

The identity and authorization of a person seeking access can be verified by such measures as:

— A PIN to activate a door control reader;
— A badge system which may also activate an electronic reader;
— A badge exchange scheme at an entry control point;
— Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive,

related information. The nature and depth of background checks should be in proportion to the security level of the source and in accordance with the State's national standards or as determined by the regulatory body.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

Regulatory provisions should ensure that the operator assesses whether those individuals with access to security information or radioactive sources are reliable. Unless determined to be trustworthy, they should not be granted unescorted access.

Security objective: Provide a security plan.

Security measures: Documentation of security arrangements and reference procedures.

Security arrangements and reference procedures should be adopted in the form of a security plan. For examples of the content of a security plan, see Appendix II.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

The security statement should include procedures for investigating and reporting any unauthorized access to or removal of a source.

Security objective: Establish a security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting of security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

— Discrepancy in accounting data;

— Suspected or actual theft of a radioactive source;
— Unauthorized intrusion into a facility or source storage area;
— Discovery of a suspected or actual explosive device in or near a facility or store;
— Loss of control over a radioactive source;
— Unauthorized access to or unauthorized use of a source;
— Other malicious acts that threaten authorized activities;
— Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
— Failure or loss of security systems that are essential to the protection of radioactive sources.

4.3.2. Performance based approach

The regulatory body may choose to specify the use of a performance based approach by which operators meet applicable security objectives. Generally, a State's choice of approach will depend on the availability of security expertise to the regulatory body and the operator. A performance based approach would function most effectively where operators have professional advisers and expertise to design and implement the necessary measures and have demonstrated a sustained record of consistency and compliance. The regulatory body should ensure that the approved measures are clearly documented, e.g. within a security plan, and assessed at appropriate intervals.

For the performance based approach, a State will need to use the national threat assessment, and may also choose to develop a DBT where applicable. The regulatory body should further specify a security objective for the classes of sources to which the performance-based approach applies. Generally, such security objectives should be stated in terms of required system effectiveness, as described in Section 3.

A security system that meets applicable security objectives should then be developed by conducting a VA against the applicable DBT or assessed threat. Depending upon the circumstances, this assessment may be performed by the regulatory body or by the operator, using the approach described in Section 3 or another methodology, as determined by the regulatory body. The results of the VA or other methodology would also be used to demonstrate that the resulting security system does, in fact, meet the applicable security objectives.

The set of security measures developed by applying the performance based approach would not necessarily correspond to the security measures for the particular source that would be recommended by the prescriptive approach listed in Tables 6–8. While measures addressing the security functions of

detection, *delay*, and *response* from Table 2 would be included, the particular combination of measures may vary in light of the situation specific analysis conducted in the VA. Application of the performance based approach generally leads to a more tailored and cost effective set of security measures than is possible using the prescriptive approach. The performance based approach does not lend itself to a statistical analysis of *deterrence* or *security management* although these functions are an integral part of the programme. Accordingly, the performance based approach should also include a requirement for deterrence and security management measures applicable to the security level of the source or sources involved, as described in the material on the prescriptive approach. The performance based approach should consider the systematic interaction of detection, delay and response in determining overall system effectiveness against the assessed threat.

System effectiveness is the key measure of the performance based approach. In order to design a security system using the performance based approach, an assumption is made that any deterrence measures will fail and that a malicious act is attempted. The security system should then be designed to achieve the required level of system effectiveness in preventing the malicious act assumed to occur in light of the assessed threat.

4.3.3. Combined approach

Many States may wish to combine aspects of both the prescriptive- and performance based approaches in order to apply security measures that meet the security objectives stated above. For example, a State could use the prescriptive approach for radioactive sources with lower potential consequences of malicious use, but apply the performance based approach to the most dangerous sources. For those most dangerous sources, the State would conduct a national threat assessment and develop a DBT. The operator would then be responsible for applying the appropriate security measures to meet a set of security objectives defined in terms of the security functions of *deterrence*, *detection*, *delay*, *response* and *security management*.

Appendix I

DESCRIPTION OF SECURITY MEASURES

Recommended security measures, some of which are referenced in Section 4, are described below.

Because national standards vary, this publication does not provide detailed advice on specifications for security equipment or physical features. However, as an overall guide, the design and reliability of security measures should be appropriate to the threat as identified by the threat assessment or as defined in the DBT. Generally, this means the use of high quality, proven equipment and technology which satisfies national or international quality standards.

I.1. ACCESS CONTROL

Access control can be exercised through entry checkpoints controlled by response personnel, the use of electronic readers or key control measures. Technology, in the form of automatic access control systems (AACSs), is available in various forms, from simple pushbutton mechanical devices to more sophisticated readers that respond to proximity tokens or individual biometric characteristics. Used with a turnstile, an AACS can also incorporate controls to inhibit practices such as 'passback' and 'tailgating'. In most cases, the use of a card should be verified by a PIN keyed into the reader and in high security situations an AACS entry point should be supervised by a guard positioned within view. The essential factor for prospective operators is to specify a viable AACS that is appropriate to the requirement and can be supported locally by a manufacturer or installer. It is also important to limit access to the AACS management computers and software to prevent unauthorized interference with the system database. Where conventional lock and key is used as a means of control, locks should be of good quality and key management procedures should be designed to prevent unauthorized access or compromise.

I.2. CAGES

Metal cages or containers may also be used to segregate and secure sources by adding another level of protection, e.g. temporary retention within a receipt and dispatch area. Elsewhere, cages could be part of the storage

arrangements within an established area that is enclosed and under control and supervision.

I.3. CCTV SURVEILLANCE

CCTV is a useful aid which allows security staff to monitor outer approaches and areas where radioactive sources are stored. Cameras can be combined with an intrusion detection system (IDS) to provide event activated camera views. However, to be fully effective, the performance of CCTV cameras and monitors should be regularly assessed to ensure that they continue to display imagery of good quality. Systems should also be supported by a response so that alarm events and indications activated by technology can be investigated.

I.4. COMMUNICATION

Security personnel at all levels should be provided with effective and reliable forms of communication. This includes communication between patrols, fixed posts and the local reporting or control centre and the communication to external agencies responsible for providing rapid response to security events.

I.5. FENCES AND GATES

The type of fence used on a perimeter should be appropriate to the threat, the nature of the sources being protected and the category of the site overall. There are various types of fence ranging from those that are little more than a demarcation to those that are more robust and can be combined with a fence mounted perimeter intrusion detection and assessment system or electrified panels. Fence lines need to be checked regularly to ensure that the fabric is in good order and free from interference or damage. Gates within a fence should be constructed to a comparable standard to the fence and secured with good quality locks.

I.6. INTRUSION DETECTION SYSTEMS

These systems are a useful means of monitoring the security of an unoccupied area. Where appropriate, the technology can be extended to the outer area of an establishment by use of a perimeter intrusion detection and assessment system. All intrusion detection systems should be supported by a response to investigate alarm events or conditions. Alarms can sound remotely at a security control point or locally through a high volume sounder. CCTV can be a useful aid in providing initial verification of events within an alarmed zone or area but should normally be backed up by a patrol making a visual check or investigation.

I.7. KEY CONTROL PROCEDURES

Keys which allow access to radioactive sources should be controlled and secured. These may be keys to cages, doors, storage containers or shielded units within which sources are used. Similar levels of control should be applied to duplicate and spare keys.

I.8. LOCKS, HINGES AND INTERLOCKS FOR DOORS

Locks used for the protection of radioactive sources should be of good quality, incorporating features that will offer some resistance to forcible attack. The same applies to hinges on doors. Keys should be safeguarded in the manner outlined above under the procedural measures. Within premises, interlock doors that meet safety requirements can serve the interests of security by controlling the movement of personnel and allowing staff to monitor access to the facility.

I.9. LOCKED, SHIELDED CONTAINERS

Shielding and fixed units containing radioactive sources can provide protection, and can delay any attempt to interfere with the source. However, when staff members are not present, the area should be covered by an intruder detection alarm system to alert the response personnel or security response of the need to investigate the circumstances of any intrusion.

I.10. MAINTENANCE AND TESTING OF SECURITY TECHNOLOGY

Considerable reliance should be placed upon security technology to provide early warning of the entry of an adversary to the site or the secured area. Intruder detection systems used for the protection of radioactive sources should therefore not only be properly specified but also tested for performance upon installation, maintained at regular intervals by competent persons, and tested at intervals specified by the regulatory body.

I.11. PASS SYSTEMS

A pass system is an efficient and cost effective means of providing a first level indication of individual authority to be within a premises or a secured area. Nevertheless, passes should be checked on entry to the facility and worn visibly by holders to confirm authority and aid identification. Embedded technology can also allow passes to be combined with use in access control systems.

I.12. QUALITY ASSURANCE

Security arrangements and procedures should be prepared, documented and maintained in line with recommended quality assurance standards such as: recording of formal approval; version control; periodic, planned review; testing of arrangements and procedures; and incorporation of lessons learned into procedures.

I.13. SECURITY AND AREA LIGHTING

Effective illumination of areas can make an important contribution to physical protection. In high security situations special lighting configurations may be necessary. However, area and street lighting that may be in place for other purposes can often provide illumination to deter intruders and assist patrolling response personnel.

I.14. SPECIALIST SECURITY DOORS AND DOOR SETS

Within certain facilities containing radioactive sources, it may be appropriate to fit storage areas with special security doors and door surrounds that offer resistance to forcible attack. This would be relevant in areas that are regularly left unattended.

I.15. STANDBY POWER

Security control rooms and security systems should be able to cope with power dips or outright loss of a main electricity supply. This can be ensured through an uninterruptible power supply and a standby generator which automatically starts when a fluctuation in power levels is detected. Battery backup has only limited duration and should, therefore, be viewed as a short term source of standby power.

I.16. WALLS

Unless they are already in place, walls are an expensive way to form a perimeter boundary. Walls also have the disadvantage of preventing response personnel from looking out beyond the protected area.

Appendix II

EXAMPLES OF CONTENT FOR A SECURITY PLAN

A security plan should include all information necessary to describe the security approach and system being used for protection of the source(s). The level of detail and depth of content should be commensurate with the security level of the source(s) covered by the plan. The following topics should typically be included:

- A description of the source, its categorization, and its use.
- A description of the environment, building and/or facility where the source is used or stored, and if appropriate a diagram of the facility layout and security system.
- The location of the building or facility relative to areas accessible to the public.
- Local security procedures.
- The objectives of the security plan for the specific building or facility, including:
  - the specific concern to be addressed: unauthorized removal, destruction, or malevolent use;
  - the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed;
  - the equipment or premises that will be secured.
- The security measures to be used, including:
  - the measures to secure, provide surveillance, provide access control, detect, delay, respond and communicate;
  - the design features to evaluate the quality of the measures against the assumed threat.
- The administrative measures to be used, including:
  - the security roles and responsibilities of management, staff and others;
  - routine and non-routine operations, including accounting for the source(s);
  - maintenance and testing of equipment;
  - determination of the trustworthiness of personnel;
  - the application of information security;
  - methods for access authorization;
  - security-related aspects of the emergency plan, including event reporting;
  - training;
  - key control procedures.

— The procedures to address increased threat level.
— The process for periodically evaluating the effectiveness of the plan and updating it accordingly.
— Any compensatory measures that may need to be used.
— References to existing regulations or standards.

Appendix III

DESCRIPTION OF A VULNERABILITY ASSESSMENT

A vulnerability assessment, also known as a security survey or security assessment, is a method for evaluating protective security systems. It is a systematic appraisal of the effectiveness of a security system for protection against an assessed threat (or DBT if one exists). The VA can be specific or general in nature, can be conducted locally by the operator or by the State/regulatory body, and can be used to help the development of regulations by the State/regulatory body or for demonstrating regulatory compliance of the operator. VAs should be performed by trained personnel. The essential elements of a VA are:

— Establishing a radioactive source inventory and associated information, taking note of the categorization, form, location and the physical environment. This process should also include disused sources;
— Assessing potential consequences associated with the unauthorized removal of the source and its malicious use or with sabotage at the facility;
— Considering the national threat assessment (or DBT, if one exists) and also any local considerations;
— Identifying existing security measures and assessing the expected effectiveness of the security system in protecting against attacks by postulated threats (and/or DBT, if one exists); and
— Determining what, if any, additional security measures are required to ensure an acceptable and proportionate level of protection.

Those conducting the VA should be technical experts familiar with the facility in question, particularly its technical and commercial imperatives, the existing security levels and safety aspects that might add to the degree of overall protection.

Appendix IV

ILLUSTRATIVE SECURITY MEASURES THAT MAY BE APPLIED TO SELECTED FACILITIES AND ACTIVITIES

This appendix is intended to support Section 4 by illustrating for the regulatory body the practical implementation of security measures for a range of relevant facilities and activities, including a mobile operation where the measures applicable to a fixed installation are not practicable. National threat assessments will vary and so security measures will need to be adjusted as appropriate.

Security function	Large fixed installation Security Level A (e.g. industrial irradiator)	Small fixed installation Security Level B (e.g. small radiography company)	Small fixed installation Security Level C (e.g. small process line)	Adjustments for mobile uses Security Level B (special case) (e.g. mobile radiography)
DETECT	Immediate detection of any unauthorized access to the secured area/source location. *Perimeter intruder detection and assessment system, and local intruder protection system or continuous surveillance by operator personnel.*	Immediate detection of any unauthorized access to the secured area/source location. *Perimeter intruder detection and assessment system, or local intruder protection system or continuous surveillance by operator personnel.*		Immediate detection of any unauthorized access to the secured area/source location. *Continuous surveillance by operator personnel.* *Vehicle alarm when source in storage.*
	Immediate detection of any attempted unauthorized removal of the source, including by insider *Verification by process control data and interlocks when source in use.* *(Local intruder alarm when source is in pool.)*	Detection of any attempted unauthorized removal of the source. *Tamper detection equipment or visual inspection.*	Detection of unauthorized removal of source. *Detection by process control data and maintenance routine.*	Detection of any attempted unauthorized removal of the source. *Tamper detection equipment or vehicle alarm or visual inspection.*
	Immediate assessment of detection. *Remote monitoring of alarms/ CCTV (by operator personnel or local police).* *Security patrol.*	Immediate assessment of detection. *Remote monitoring of alarms or CCTV (by operator personnel or local police).*	Immediate assessment of detection *Visual inspection.*	Immediate assessment of detection *Operator personnel.* *(Client personnel if on a job site.)*

Security function	Large fixed installation Security Level A (e.g. industrial irradiator)	Small fixed installation Security Level B (e.g. small radiography company)	Small fixed installation Security Level C (e.g. small process line)	Adjustments for mobile uses Security Level B (special case) (e.g. mobile radiography)
DETECT	Immediate communication to response personnel. *Landline and one of:* *Private mobile radio.* *Cellphone.* *Pager.*	Immediate communication to response personnel. *Landline.* *Cellphone.*		Immediate communication to response personnel. *Cellphone, and /or* *private mobile radio.* *Landline if on a job site.*
	Means to detect loss of source through verification. *Verification by process control data and interlocks when source in use.* *(Local intruder alarm when source is in pool.)*	Means to detect loss of source through verification. *Verification by use of safety instrumentation.*	Means to detect loss of source through verification. *Verification by process control data and use of safety instrumentation for source in storage.*	Means to detect loss of source through verification. *Verification by use of safety instrumentation, and* *visual inspection.*
DELAY	Delay after detection sufficient for response personnel to interrupt the unauthorized removal .	Delay to minimize likelihood of unauthorized removal.	Delay to reduce the likelihood of unauthorized\ed removal.	Delay to minimize likelihood of unauthorized removal.
	Exterior wall. *Locks on process control panel/ interlocks.* *Locked storage of process tools (or keep off-site).* *Security final door and door set.*	*Exterior wall* *Locks on radiography cell/ interlocks.* *Locked storage of tools.* *Security door and door set.* *Out of hours: secure source store or bunker.*	*One barrier such as cage or housing and secure fixings.*	*Continuous surveillance by operator personnel.* *Locks on source container.* *Source container secured to vehicle.* *Locked storage of tools.* *Out of hours: vehicle locked and alarmed.*

Security function	Large fixed installation Security Level A (e.g. industrial irradiator)	Small fixed installation Security Level B (e.g. small radiography company)	Small fixed installation Security Level C (e.g. small process line)	Adjustments for mobile uses Security Level B (special case) (e.g. mobile radiography)
RESPONSE	Immediate response to assessed alarm with sufficient resources to interrupt and prevent unauthorized removal. *Operator personnel.* *Police response.*	Immediate initiation of response to interrupt. *Operator personnel.* *Police response.*	Appropriate action in the event of unauthorized removal of source. *Operator personnel.* *Police response.*	Immediate initiation of response to interrupt. *Operator personnel.* *Police response.*
SECURITY MANAGEMENT	Access controls to source location that effectively restrict access to authorized persons only. *Pass system or identification and verification by recognition of operator personnel*	Access controls to source location that effectively restrict access to authorized persons only. *Recognition by operator personnel.* *Locks to suitable specification.* *Key management (safe, procedure etc.).*	Access controls to source location that effectively restrict access to authorized persons only. *One barrier such as cage or housing and secure fixings.*	Access controls to source location that effectively restrict access to authorized persons only. *Recognition by operator personnel* *Vehicle locks to suitable specification.* *Keys kept with authorized personnel.*
	Trustworthiness of authorized individuals. *Periodic background check of operator personnel in accordance with national policy.*	Trustworthiness of authorized individuals. *Periodic background check of operator personnel in accordance with national policy.*	Trustworthiness of authorized individuals. *Background check of operator personnel involved in management of source in accordance with national policy.*	Trustworthiness of authorized individuals. *Periodic background check of operator personnel in accordance with national policy.*

Security function	Large fixed installation Security Level A (e.g. industrial irradiator)	Small fixed installation Security Level B (e.g. small radiography company)	Small fixed installation Security Level C (e.g. small process line)	Adjustments for mobile uses Security Level B (special case) (e.g. mobile radiography)
SECURITY MANAGEMENT	Identify and protect sensitive information. *Promotion of security culture.* *Relevant staff induction.* *Roles and responsibilities.* *Inventory protected.* *Security plan.* *Security management procedures.* *Security containers.*	Identify and protect sensitive information. *Promotion of security culture.* *Relevant staff induction.* *Roles and responsibilities.* *Inventory protected.* *Security plan.* *Security management procedures.* *Security containers.*	Identify and protect sensitive information. *Promotion of security culture.* *Relevant staff induction.* *Roles and responsibilities.* *Inventory protected.* *Security plan.* *Security management procedures.* *Security containers (locked cabinet).*	Identify and protect sensitive information. *Promotion of security culture.* *Relevant staff induction.* *Roles and responsibilities.* *Inventory protected (at home base).* *Security plan.* *Security management procedures.* *Security containers (at home base).*
	Security plan. *Security plan consistent with Appendix II.*	Security plan. *Security plan consistent with Appendix II.*	Security plan. *Security statement consistent with Appendix II.*	Security plan. *Security plan consistent with Appendix II.*

Security function	Large fixed installation Security Level A (e.g. industrial irradiator)	Small fixed installation Security Level B (e.g. small radiography company)	Small fixed installation Security Level C (e.g. small process line)	Adjustments for mobile uses Security Level B (special case) (e.g. mobile radiography)
SECURITY MANAGEMENT	Capability to manage security events covered by security contingency plans. *Staff induction/training/awareness briefing.* *Security contingency plan (part of security plan).* *Lessons learned feedback sessions.* *Occasional exercises of security contingency plan.* *Review of security contingency plan.*	Capability to manage security events covered by security contingency plans. *Staff induction/training/awareness briefing.* *Security contingency plan (part of security plan).* *Lessons learned feedback sessions.* *Evidence of periodic liaison with local police.* *Review of security contingency plan.*	Capability to manage security events covered by security contingency plans. *Staff induction/training/awareness briefing.* *Security contingency plan (part of security plan)* *Review of security contingency plan for maintenance periods and annually for operations.*	Capability to manage security events covered by security contingency plans. *Staff induction/training/awareness briefing.* *Security contingency plan (part of security plan).* *Lessons learned feedback sessions.* *Evidence of once per visit liaison with local police.* *Review of security contingency plan.*
	Security event reporting system. *Identified responsibilities for reporting (in security plan).* *Immediate verbal reports prompt follow-up written reports included in security plan.* *Demonstrable clarity on reporting route.*	Security event reporting system. *Identified responsibilities for reporting (in security plan).* *Immediate verbal reports prompt follow-up written reports included in security plan.* *Demonstrable clarity on reporting route.*	Security event reporting system. *Identified responsibilities for reporting (in security plan).* *Immediate verbal reports prompt follow-up written reports included in security plan.* *Demonstrable clarity on reporting route.*	Security event reporting system. *Identified responsibilities for reporting (in security plan).* *Immediate verbal reports prompt follow-up written reports included in security plan.* *Demonstrable clarity on reporting route.*

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources (Interim Guidance for Comment), IAEA-TECDOC-1355, IAEA, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Radiation Generators, IAEA Safety Standards Series No. RS-G-1.10, IAEA, Vienna (2007).

[5] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

[6] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles IAEA Safety Standards Series No SF-1, IAEA, Vienna (2006).

[7] International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations, New York (2005).

[8] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); CPPNM Amendment, GOV/INF/2005/10–GC(49)/INF/6, IAEA, Vienna (2005).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Remediation of Areas Contaminated by Past Activities and Accidents Safety Requirement, IAEA Safety Standards Series No. WS-R-3, IAEA, Vienna (2003).

[11] INTERNATIONAL COMMISION ON RADIOLOGICAL PROTECTION, Protecting People against Radiation Exposure in the Event of A Radiological Attack Publication 96, Pergamon Press, Oxford (2005).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport, IAEA Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (EPR-D-Values), IAEA, Vienna (2006).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007), http://www-ns.iaea.org/standards/safety-glossary.html.
[19] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

DEFINITIONS

authorization. A permission granted in a document by a regulatory body to a person who has submitted an application to manage a radioactive source. The authorization can take the form of a registration, a licence or alternative effective legal control measures which achieve the objectives of the Code of Conduct (adopted from Ref. [1]).

design basis threat. A comprehensive description of the motivations, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated (adapted from Ref. [13]).

disused source. A radioactive source which is no longer used, and is not intended to be used, in facilities and activities for which authorization has been granted (adopted from Ref. [18]).

malicious act. A wrongful act or activity intentionally done or engaged in without legal justification or excuse (e.g. smuggling) or an act or activity intended to cause death or physical injury to any person, material damage to any person (e.g. theft) or damage to property or to the environment (adopted from GOV/2002/10).

operator. Any organization or person applying for authorization or authorized and/or responsible for nuclear, radiation, radioactive waste, or transport safety when undertaking activities or in relation to any nuclear facilities or sources of ionizing radiation. This includes private individuals, governmental bodies, consignors or carriers, licensees, hospitals, self-employed persons, etc. (adopted from Ref. [18]).

radioactive source. Radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It also means any radioactive material released if the radioactive source is leaking or broken, but does not mean material encapsulated for disposal, or nuclear material within the nuclear fuel cycles of research and power reactors (adopted from Ref. [1]).

regulatory body. An entity or organization or a system of entities or organizations designated by the government of a State as having legal authority for exercising regulatory control with respect to radioactive sources, including issuing authorizations, and thereby regulating one or more aspects of the safety or security of radioactive sources (adopted from Ref. [1]).

sabotage. Deliberate damage; sabotage in this context means deliberate damage to a radioactive source in use, storage or transport or to an associated facility. A deliberate act directed against a radioactive source in use, storage or transport could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive material (adapted from Ref. [19]).

(nuclear) security. The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities (adopted from Ref. [12]).

security culture. The characteristics and attitudes in organizations and of individuals which establish that security issues receive the attention warranted by their significance (adopted from Ref. [1]).

security contingency plan. A part of the security plan or a stand-alone document that identifies reasonably foreseeable security events, provides initial planned actions, (including alerting appropriate authorities) and assigns responsibilities to appropriate operator personnel and response personnel.

security plan. A document — prepared by the operator and possibly required to be reviewed by the regulatory body — that presents a detailed description of the security arrangements in place at a facility.

storage. The holding of radioactive sources in a facility that provides for their containment with the intention of retrieval (adopted from Ref. [1]).

threat assessment. An analysis that documents the credible motivations, intentions and capabilities of potential adversaries that could cause undesirable consequences with regard to radioactive material in use or storage and its associated facilities (adopted from Ref. [12]).

unauthorized removal. The theft or other unlawful taking of radioactive sources (adapted from Ref. [19]).

vulnerability assessment (VA). A process which evaluates and documents the features and effectiveness of the overall security system at a particular facility.

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10 (Implementing Guide)
STI/PUB/ 1386 (40 pp.; 2008)
ISBN 978-92-0-102509-8 Price: €20.00

SECURITY IN THE TRANSPORT OF RADIOACTIVE MATERIAL
IAEA Nuclear Security Series No. 9 (Implementing Guide)
STI/PUB/1348 (39 pp.; 2008)
ISBN 978-92-0-107908-4 Price: €20.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8 (Implementing Guide)
STI/PUB/1359 (25 pp.; 2008)
ISBN 978-92-0-109908-2 Price: €20.00

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7 (Implementing Guide)
STI/PUB/1347 (37 pp.; 2008)
ISBN 978-92-0-107808-7 Price: €30.00

CATEGORIZATION OF RADIOACTIVE SOURCES
IAEA Safety Standards Series No. RS-G-1.9 (Safety Guide)
STI/PUB/1227 (55 pp.; 2005)
ISBN 92-0-103905-0 Price: €18.00

SAFETY OF RADIATION GENERATORS AND SEALED RADIOACTIVE SOURCES
IAEA Safety Standards Series No. RS-G-1.10 (Safety Guide)
STI/PUB/1258 (59 pp.; 2006)
ISBN 92-0-107506-5 Price: €25.00

INTERNATIONAL BASIC SAFETY STANDARDS FOR PROTECTION AGAINST IONIZING RADIATION AND FOR THE SAFETY OF RADIATION SOURCES
Safety Series No. 115
STI/PUB/996 (353 pp.; 1996)
ISBN 92-0-104295-7 Price: €78.50

CODE OF CONDUCT ON THE SAFETY AND SECURITY OF RADIOACTIVE SOURCES
IAEA/CODEOC/2004 (122 pp.; 2004) Price: Cost free

SECURITY OF RADIOACTIVE SOURCES (INTERIM GUIDANCE FOR COMMENT)
IAEA-TECDOC-1355
ISBN 92-0-105203-0 Price: €15.00

This report provides guidance and recommended measures for the prevention, detection and response to malicious acts involving radioactive sources. It is intended to help prevent the loss of control of such sources. It also recommends that security measures be applied to radioactive sources in manufacture, use and short term or long term storage. This Implementing Guide recommends that security measures be applied on a graded basis, taking into account the current evaluation of the threat, the relative attractiveness of the source, and the potential consequences resulting from malicious use. The requisite level of security is achieved through a combination of deterrence, detection, delay, response and security management.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102609–5
ISSN 1816–9317