IAEA-TECDOC-1355

Security of radioactive sources

Interim guidance for comment

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

June 2003

The originating Section of this publication in the IAEA was:

Radiation Safety Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

SECURITY OF RADIOACTIVE SOURCES:
INTERIM GUIDANCE FOR COMMENT
IAEA, VIENNA, 2003
IAEA-TECDOC-1355
ISBN 92–0–105203–0
ISSN 1011–4289

Printed by the IAEA in Austria
June 2003

FOREWORD

In previous IAEA publications, there have been only rather general security requirements for non-nuclear radioactive material. These requirements were primarily directed to such issues as unintentional exposure to radiation, negligence and inadvertent loss. However, it is clear that more guidance is needed to not only try and prevent further events involving orphan sources, but also to prevent the deliberate attempt to acquire radioactive sources for malevolent purposes.

Member States have requested guidance on the type and nature of security measures that might be put in place and on the methodology to be used in choosing such measures. These requests were also endorsed in the findings of the international conference on “Security of Radioactive Sources” held in March 2003.

Practical advice on assessing and implementing security measures complements the general commitments in the proposed Revised Code of Conduct on Safety and Security of radioactive Sources.

A Safety Guide entitled “Safety and Security of Radiation Sources” that, amongst other things, discusses these issues is being drafted. However, it is recognized that guidance material is required before this document will be finalized in order to allow Member States opportunity to put in place appropriate actions and planning to address current issues.

Hence the purpose of the current document is to provide advice on security approaches and to allow comment on detailed recommendations for levels of security on radioactive sources that may be incorporated within the Safety Guide.

The IAEA officers responsible for this publication were R. Cameron and B. Dodd of the Division of Radiation and Waste Safety.

EDITORIAL NOTE

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

Unsecured sources are causing deaths and serious injuries in many parts of the world. The IAEA has published a number of reports that describe the human health consequences of uncontrolled sources [1–5]. In addition to these considerations, the economic losses can be considerable. It has been reported that *"In total, the direct and indirect costs in Mexico for the remedial actions after the accident in 1983, when a teletherapy source was accidentally melted, is estimated to be about 34 million US dollars"* [6].

The question of safety and security of sources has been discussed several times by the IAEA's Board of Governors. In a resolution (GC(42)/RES/12) on "The safety of radiation sources and the security of radioactive materials", adopted on 25 September 1998, the General Conference — inter alia — encouraged all governments *"to take steps to ensure the existence within their territories of effective national systems of control for ensuring the safety of radiation sources and the security of radioactive materials"*.

The International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (BSS) [7] specifically requires [para. 2.34] that:

> *"Sources shall be kept secure so as to prevent theft or damage and to prevent any unauthorized legal person from carrying out any of the actions specified in the General Obligations for practices of the Standards (see paras 2.7–2.9), by ensuring that:*
>
> *(a) control of a source not be relinquished without compliance with all relevant requirements specified in the registration or licence and without immediate communication to the Regulatory Authority, and when applicable to the relevant Sponsoring Organization, of information regarding any decontrolled, lost, stolen or missing source;*
>
> *(b) a source not be transferred unless the receiver possesses a valid authorization; and*
>
> *(c) a periodic inventory of movable sources be conducted at appropriate intervals to confirm that they are in their assigned locations and are secure."*

However, before 11 September 2001, the security of radioactive sources was largely addressed by measures protecting the sources from unintentional access by inappropriately qualified personnel or attempts at theft for financial gain. This assumption has now had to be modified to also include the need to prevent access to certain sources by people deliberately and malevolently seeking to cause radiation exposure or dispersal of radioactive materials. One known case of an attempt to malevolently use radioactive material occurred in 1995 when Chechens placed a container with ^{137}Cs in a Moscow park [8]. Fortunately, the material was not dispersed. In a news article [9] regarding a difference case, it was reported that *"six Lithuanian nationals were arrested in the Lithuanian capital, Vilnius, in a raid…during which a large amount of radioactive metal, ^{137}Cs, was confiscated."*

The need for the development of further guidance on the security of radioactive sources was recognized by the Board of Governors and incorporated into the IAEA's Nuclear Security Plan of Action that was approved in principle by the Board in March 2002.

Efforts were also made in the revision to the Code of Conduct on the Safety and Security of Radioactive Sources [10] to address security issues in more depth. The Code states that:

"Every State should, in order to protect individuals, society and the environment, take the appropriate measures necessary to ensure:

(a) that the radioactive sources within its territory, or under its jurisdiction or control, are safely managed and securely protected during their useful lives and at the end of their useful lives; and

(b) the promotion of safety culture and of security culture."

1.2. Purpose

This report is primarily addressed to Regulatory Authorities but it is also intended to provide guidance to manufacturers, suppliers and users of sources. Its objective is to assist Member States in deciding which security measures are needed to ensure consistency with the International Basic Safety Standards [7] and the Revised Code of Conduct for the Safety and Security of Radioactive Sources [10]. It is recognized that there must be a balance between managing sources safely and securely, while still enabling them to be used by authorized personnel without undue hindrance. Thus the level of security should be commensurate with the potential hazard posed by the source, recognizing the need to ensure appropriate use of the source for beneficial purposes.

To ensure security of sources requires that measures be applied to prevent unauthorized access to radioactive sources at all stages of their life cycle, as well as loss, theft, and unauthorized transfer of sources. To ensure the safety of radioactive sources requires controlling exposure to radiation from sources, both directly and as a consequence of incidents, so that the likelihood of harm attributable to such exposure is very low. Security is therefore a prerequisite for safety. Hence safety and security aspects of sources are intimately linked and many of the measures designed to address one, will also address the other. For this reason, the safety measures and procedures already in place for some sources may already meet basic security needs. However, consideration does need to be given to the expansion of these to take into account the threat of people acquiring control of a radioactive source for malevolent purposes.

It is recognized that the measures recommended in this document and implemented for safety and security purposes may not protect radioactive sources from all possible efforts by a group of committed persons to gain control over them. However, it is possible to make it more difficult for such a group by prudent design of such measures. A graded concept of security measures is outlined that is based on the potential hazard and the vulnerability of the source or the device, as well as the potential consequences of malevolent actions. It is believed that implementation of these measures will lower the risk of such consequences associated with the source by minimizing the likelihood of unauthorized acquisition.

The recommended security measures are aimed at the prevention and countering of malevolent acts by a combination of deterrence, early detection and delay of attempts at unauthorized acquisition, mitigation of consequences by timely detection and appropriate measures to respond to a loss of authorized control, including recovery. However, this report does not detail all of these aspects, since some are covered in other documents.

1.3. Scope

A complete programme aimed at addressing the malevolent use of radioactive sources needs to consider a large range of issues including: the appropriate design and manufacture of sources; the various means of acquisition of sources; the prevention of use of any sources acquired; and the mitigation of the impacts if sources are used maliciously. This document

only covers the processes to determine what level of security is required for sources throughout their lifecycle, and the assignment of security measures to sources based on graded performance requirements to deter, detect, and, if necessary respond to theft of radioactive material. In doing so, it is recognized that such measures will also minimize inadvertent or negligent losses of sources.

While security considerations for all radioactive sources are outlined in this document, the main focus is on radioactive sources that could be dangerous if they are not under control (primarily Categories 1 to 3 in Ref. [11]). Additionally, the security concerns addressed in this report relate primarily to sealed sources; however, consistent with the Revised Code of Conduct [10], the scope of this document also includes any radioactive material released if the source is leaking or broken.

These recommendations do not cover the security of nuclear material since this is addressed in other publications [12, 13]. However, plutonium in sources such as PuBe neutron sources is included.

It is not the intent of this report to duplicate, replace, or supersede existing recommendations but only to amplify on radioactive source security. Therefore, it does not specifically discuss the radiation safety requirements, which are outlined in other IAEA documents and should be followed in addition to the security requirements. Again it is recognized that some measures address both safety and security concerns.

The process proposed in this report is applicable to the complete life cycle of sources including: manufacture, supply, receipt, storage, use, transfer, import, export, transport, maintenance or disposal of radioactive sources. However, detailed information on transport will be addressed in further publications. As in the Revised Code of Conduct on the Safety and Security of Radioactive Sources [10], these are all generically termed ‘management’ of sources (see definitions).

Facilities covered in this report are those areas where radioactive sources are managed and include such places as: (a) fixed industrial radiography installations; (b) irradiation facilities; (c) treatment rooms where radiotherapy sources are used; and (d) source storage locations. These security measures are also applicable to radioactive sources in nuclear facilities or radioactive waste disposal facilities, recognizing that these already should provide a high standard of security based on the existing requirements for physical protection against unauthorized removal of nuclear material and acts of sabotage.

1.4. Definitions

Accounting means physically checking that all sources are present in their expected location. This may be satisfied by an appropriate radiation survey.

Design basis threat for sources means the attributes and characteristics of potential insider and/or external adversaries, who might attempt damage to, or unauthorized removal of, radioactive sources , against which a physical protection system is designed and evaluated.

Inventorying means a campaign to physically check all sources possessed, by specifically and uniquely identifying each individual source using appropriate means such as serial numbers.

Management means all activities, administrative and operational, that are involved in the manufacture, supply, receipt, storage, use, transfer, import, export, transport, maintenance or disposal of radioactive sources [10].

Nuclear material means plutonium except that with isotopic concentration exceeding 80% in ^{238}Pu; ^{233}U; uranium enriched in isotope 235 or, uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue; any material containing one or more of the foregoing.

Principal parties means the persons having the main responsibilities for the application of the Basic Safety Standards. These are: (a) registrants or licensees and (b) employers [7].

Safety means measures intended to minimize the likelihood of accidents with radioactive sources and, should such an accident occur, to mitigate its consequences [10].

Safety culture means the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance [10].

Security means measures to prevent unauthorized access or damage to, and loss, theft or unauthorized transfer of, radioactive sources [10].

Security culture means characteristics and attitudes in organizations and of individuals, which establish that security issues receive the attention warranted by their significance [10].

2. SECURITY DESIGN AND EVALUATION

2.1. Overall strategy

In attempting to address the threats from malevolent acts involving radioactive sources, it is clear that sources of certain magnitudes and types are more attractive to those with malevolent intent than others. Therefore, the approach to security needs to be graded accordingly. There are several components of a complete overall strategy:

(1) Appropriate manufacture and design of sources and devices to minimize the feasibility of malicious actions and maximize security.

(2) Management of sources only within an authorized, regulated, legal framework. Amongst other things, this includes efforts to:

   (a) provide a strong regulatory infrastructure;
   (b) prevent the unauthorized production of radioactive material;
   (c) validate legal purchases and ensure adequate justification for possession of sources;
   (d) ensure the reliability of personnel involved in managing sources.

(3) Prevention of acquisition of radioactive sources by those with malevolent intent. This includes measures to:

   (a) deter unauthorized access to the source, or source location, in order to deter theft;
   (b) detect any such attempts at unauthorized access;
   (c) delay unauthorized access or theft;
   (d) provide rapid response to attempts at unauthorized access or theft.

(4) Detection of actual theft or loss in order to appropriately respond and allow recovery efforts to start as soon as possible. This includes:

   (a) radiation, or other alarms;
   (b) accounting and inventorying.

(5) Efforts to recover any stolen or lost sources and bring them into secure regulatory control.

(6) Prevention of use for unauthorized purposes of any sources acquired improperly.

(7) Minimization of the accidental or malevolent consequences of any use.

This document primarily addresses the second, third and fourth points above. Other existing, and future, IAEA publications cover the rest of the topics [14–18].

2.2. Threat assessment

The use of a design basis threat (see definition) assessment methodology is recommended as the best method to design the security measures for specific sources. The design basis threat will vary quite widely according to the country, facility and source. Associated security measures should be commensurate with the threat and the level of risk acceptance. Threat assessments can range from being very detailed to quite generic.

Security measures, likewise, can be very specific or based on generic assessments performed at an organizational or government level. At one extreme, security requirements might be based only on the consequences of malevolent actions without an assessment of the likelihood of the threat (see Section 2.4).

A detailed threat assessment provides the means of adjusting security provisions in accordance with the results of that analysis and more specifically addressing the potential consequences associated with loss of control over each specific source.

A detailed design basis threat assessment methodology to define the appropriate level of security consists of the following activities, which are also described in the flowchart in Appendix I.

(1) Characterize the source, its type, nature and application (identify the target).

(2) Perform an assessment of the potential threat within the country as a whole, based on information from security and intelligence experts.

(3) Evaluate the potential consequences of successful actions to acquire the source. This can range from theft with the intention to threaten action in order to cause panic, through to the deployment of a radiological dispersal device and the attendant consequences.

(4) Determine, based on the assessment of threat and potential consequences, a design basis threat against which the security should be designed and evaluated. For example, the threat may range from attempts by one person to gain access but without any special equipment through to a well-equipped and possibly armed group.

(5) Perform a vulnerability analysis for the specific source, or sources against this design basis threat.

(6) If there is a requirement to reduce the risk associated with unauthorized access and acquisition, then first optimize existing measures and then implement additional measures.

As noted, many of these measures may just be extensions or amplifications of the existing safety measures. Appendix II gives a brief, hypothetical example of the application of the design basis threat assessment method.

2.3. Performance objectives for security groups

Based on the vulnerability analysis for a specific source, an assessment of the risk can be made. The level of this risk will determine the security measures required to protect the source. The higher the risk, the more capability will be required from the security systems.

This level of capability can be expressed as performance objectives on the security system. While there is a wide range of possible security measures, they can be described by their capability to deter, to detect and to delay unauthorized access or acquisition.

In this section, four security groups are defined based on these fundamental protection capabilities. They provide a systematic way of categorizing the graded performance objectives required to cover the range of security measures that might be needed, depending on the assessed risk.

These security groups categorize the performance objectives of a security system as follows:

— **Security Group A:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible.

— **Security Group B:** Measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner.

— **Security Group C:** Measures should be established to deter unauthorized access and verify the presence of the source at set intervals.

— **Security Group D:** Measures should be established to ensure safe use of the source and adequately protect it as an asset, verifying its presence at set intervals.

Table 1. Summary of security group performance objectives

<table>
<tr><th>Security Group A</th><th>Security Group B</th><th>Security Group C</th><th>Security Group D</th></tr>
<tr><td colspan="4">Safe management and protect as an asset</td></tr>
<tr><td colspan="3">Deter unauthorized access</td><td rowspan="4"></td></tr>
<tr><td colspan="2">Timely detection of unauthorized access</td><td rowspan="3">Verification of source presence at set intervals.</td></tr>
<tr><td colspan="2">Timely detection of unauthorized acquisition of the radioactive source</td></tr>
<tr><td>Delay acquisition until response is possible</td><td></td></tr>
</table>

The choice of the quality and effectiveness of the measures that give effect to the above requirements will be related to the specific design basis threat.

Protection against unauthorized access for security reasons is primarily aimed at trying to prevent theft of the material. Measures to achieve the same objective may already be in place for safety reasons to protect against unintentional radiation exposure.

2.4. Assignment of radioactive sources to security groups

The assignment of a radioactive source to a security group is most effectively achieved by using the outcomes of the threat assessment. This allows most flexibility and specificity to account for the variability in threat levels and security environments within Member States. It also permits different choices of security groups for sources in the different stages of their life cycle. Alternatively some countries may perform countrywide threat and vulnerability assessments and make allocations of sources to security groups based on these assessments.

In the event that insufficient data are available to perform a reasonable design basis threat assessment, or it is not considered desirable or necessary to do so, then security measures could be based upon the *consequences* of the malevolent acquisition and use of the source(s), and an assumed threat to the source. The IAEA has developed a revised Categorization of Radioactive Sources [11] that could be used for this first purpose, since it uses as its basis the potential human health impact of uncontrolled sources and provides a measure of the inherent hazard associated with the source. However, it should be recognized that it contains no consideration of the social or economic impacts of the loss of control of the sources.

In the revised categorization, sources are divided into five categories, with Category 1 being the most significant and Category 5 the least. Sources in Categories 1 to 3 generally have the possibility of giving rise to exposure sufficient to cause severe deterministic effects if they are uncontrolled. A severe deterministic effect is one that is fatal or life threatening or results in permanent injury that decreases the quality of life.

Consistent with the Revised Code of Conduct, each of the categories includes the radioactive material released if any of the sources in the group is leaking or broken. The categorization methodology also allows for aggregation of sources in one location.

The security grouping of sources given in Table 2. is based upon the revised categorization along with the implicit assumption of a threat by a person or group with serious intent to acquire the source. This latter assumption is used as a generic design basis threat. These assignments are put forward as default assignments. Different circumstances or more detailed assessments may justify moving a source up or down a security group. One reason for a source being categorized in a higher security group could be that the specific threat assessment may reveal that some facilities with sources or some mobile sources are more vulnerable to acquisition, even though they may not be the highest activity sources.

However the assignment is made, either by use of threat assessment techniques or using the default assignment in Table 2, then it is possible to decide on some specific security measures that will meet the performance objectives for that group.

Table 2. Security groups based upon source categorization

Security Group	Source Category	Examples of practices
A	1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy Fixed multi-beam teletherapy (gamma knife)
B	2	Industrial radiography High/medium dose rate brachytherapy
	3	Fixed industrial gauges (e.g. level, dredger, conveyor) Well logging gauges
C	4	Low dose rate brachytherapy (except those below) Thickness/fill-level gauges Portable gauges (e.g. moisture/density) Bone densitometers Static eliminators
D	5	Low dose rate brachytherapy eye plaques and permanent implant sources X ray fluorescence devices Electron capture devices

3. TYPES OF SPECIFIC SECURITY MEASURES

The security performance objectives for the groups will be met by the use of a combination of administrative and technical measures. These security measures should be seen as an integrated concept of safety and security involving industrial safety arrangements, radiation protection measures and appropriate design to achieve the necessary level of protection against unauthorized acquisition of radioactive sources. Guidance on the application of these measures is given in Sections 4 and 5.

3.1. Administrative measures

Administrative measures are the use of policies, procedures, and practices that direct personnel to securely and safely manage sources. Administrative measures are used to support or supplement the technical ones. Administrative measures include:

— access control procedures;
— alarmed access points (e.g. with radiation detectors);
— key control procedures;

— video cameras or personal surveillance;
— records related to management of sources;
— inventories;
— regulations and guidance;
— reliability and trustworthiness of personnel;
— information security;
— quality assurance measures; and
— establishment of a safety culture and a security culture.

Even if surveillance measures involve intrusion detectors as opposed to human observation, they are considered administrative measures in that they do not provide a physical barrier.

3.2. Technical measures

Technical measures pose a physical barrier to the radioactive source, device or facility in order to separate it from unauthorized personnel and to deter, or to prevent, inadvertent or unauthorized access to, or removal of, a radioactive source.

Technical measures are generally hardware or security devices and include:

— fences;
— walls;
— cages;
— transport packagings;
— locks and interlocks for doors;
— locked, shielded containers; and
— intrusion-resistent source-holding devices.

It is inappropriate for this report to give detailed specifications for technical measures; however, their design and level of quality assurance should be appropriate to the threat and the potential consequences of the defined malevolent act. Generally, this means high quality materials and components [19–22].

4. GENERAL ADMINISTRATIVE MEASURES

Regardless of the security group, there are a number of recommended general administrative measures that are common for the management of all sources. These are covered in this section, while the administrative and technical measures that are graded according to each security group are given in Section 5.

The Revised Code of Conduct on the Safety and Security of Radioactive Sources [10] and the basic tenets of physical protection espouse many general provisions that will contribute to the security of sources. Some of these general principles for establishing security measures are summarized in the following:

(1) The State is responsible for the establishment, implementation and maintenance of a security regime by establishing and maintaining a regulatory framework to govern the implementation of security measures.

(2) The State should establish or designate a Regulatory Authority, which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities.

(3) All organizations involved in implementing security measures should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.

(4) The security measures should be based on an evaluation of the threat and potential consequences.

(5) Emergency plans to respond to the loss of authorized control of higher risk radioactive sources should be prepared and appropriately exercised by all authorized owners and authorities concerned.

(6) Authorized owners and authorities should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the security measures.

4.1. Responsibilities and authorities

4.1.1. Regulatory Authority

The IAEA has issued a publication that details the *"requirements for legal and governmental responsibilities in respect of the safety of nuclear facilities, the safe use of sources of ionizing radiation, radiation protection, the safe management of radioactive waste and the safe transport of radioactive material"* [23]. Further relevant Regulatory Authority responsibilities can be found in the Revised Code of Conduct [10]. Hence, this section just highlights some of the more important considerations.

The Regulatory Authority should require that those who intend to manage radioactive sources seek an authorization, unless exempted or only notification is used. The Regulatory Authority should establish a formal, documented process to evaluate applications requesting the possession and use of radioactive sources. Since those with malevolent intent may attempt legal purchases, it is important from a security viewpoint to be assured that requests for authorization have validity. Hence, prior to issuing any authorizations, including any authorization to purchase or sell sources, the Regulatory Authority should verify that the applicant has legitimacy, that there is an adequate justification for the management of the radioactive source as well as an adequate justification for the types and quantities of the radioactive sources requested. This procedure should be seen as an important principle applicable to the management of all kinds of radioactive sources.

In addition, and depending on the security group, the Regulatory Authority should be proactive in obtaining all relevant information and require that those who intend to use radioactive sources submit an assessment of the security of the source and/or the facility in which it is to be managed. The security assessment, based on the regulatory framework, should demonstrate the balance needed between security measures and the need to use the sources. The assessment should take into account the risk posed by the possession and use of the radioactive source. This will mean that the assessment should be more comprehensive for sources in the higher groups. The information provided should detail, among other things,

which security measures would be implemented and how the trustworthiness of individuals would be ensured.

The Regulatory Authority should also ensure that before the receipt of a radioactive source is authorized, the security provisions are in place and that arrangements have been made for its secure protection once it has become a disused source. This includes appropriate financial provisions.

The Regulatory Authority should:

— maintain appropriate records of holders of authorizations in respect of radioactive sources, with a clear indication of the type(s) of the radioactive sources that they have been authorized to use, and appropriate records for transfer and disposal of the radioactive sources on termination of the authorization;

— establish systems for ensuring that, where practicable, radioactive sources are identifiable and traceable, or where this is not practicable, ensure that alternative processes for identifying and tracing sources are in place;

— ensure that the regulatory principles and criteria with regard to the security of the radioactive sources remain adequate and valid and take into account, as applicable, operating experience and internationally endorsed standards and recommendations;

— implement an inspection programme to verify that facilities and programmes are maintained to adequately manage the radioactive sources.

4.1.2. Principal party

Registrants and licensees bear the responsibility for setting up and implementing the technical and organizational measures that are needed for ensuring both the safety and security of the sources for which they are authorized. They may appoint other people to carry out actions and tasks related to these responsibilities, but they retain the responsibility for the actions and tasks themselves. However, they should identify the specific individual(s) responsible for ensuring sources are secured in accordance with the recommendations in this report, or applicable national guidance, as well as compliance with the BSS [7] (para. 2.15). The principal party should ensure that these responsible individuals meet the requirements for training and trustworthiness set by the Regulatory Authority[1].

The principal party should ensure that:

— sources are managed in accordance with the authorization;

— when sources are not in use, they are promptly stored in an approved manner. Storage should be in accordance with the requirements for the group to which the source belongs;

[1] In principle, the requirements of a State's Regulatory Authority should be followed regarding safety and security of radioactive sources; however, in the absence or inadequacy of such regulations, IAEA standards, recommendations and guidance should be used.

— any transfer of sources to another person is documented and that person is authorized in accordance with the applicable regulatory requirements to receive the transferred source;

— financial provisions in accordance with the regulatory requirements for the safe management of disused sources are in place;

— sources are shipped and received in accordance with regulatory requirements.

The principal party and the authorized persons identified by the principal party should be prepared to assist State authorities or local law enforcement authorities in recovering any lost or stolen source.

4.1.3. Individuals with assigned responsibility for sources

A responsible individual should have the authority to ensure that the requirements for security of sources given in this report are implemented. The responsible individual should ensure that all personnel who use or have access to the sources:

— are reliable;
— are authorized;
— have the proper training consistent with their duties in handling those sources.

4.2. Inventories and records

All sources should be inventoried at least on an annual basis, or in accordance with other applicable regulatory requirements. The records should be appropriately secured.

Source records should be maintained and updated following:

— the routine inventory;
— whenever the recorded parameters change; and particularly,
— whenever sources are transferred.

The records should include the following particulars:

— location of the source;
— radionuclide;
— radioactivity on a specified date;
— serial number or unique identifier;
— physical form;
— source use history (e.g. logging all source handling operations); and
— receipt, transfer or disposal of the source.

Sources should be accounted for by recording all source movements into and out of the storage area.

4.3. Status and event reporting system

The principal party should ensure that there is a procedure for communicating to the Regulatory Authority the information required by the source grouping or by the need for national or other registries.

In addition to normal reporting requirements relating to safety issues, reports of unusual events that may affect security should be reported promptly. Unusual events to be reported to the Regulatory Authority could include:

- loss of control over a radioactive source;
- unauthorized access to, or unauthorized use of, a source;
- malicious acts threatening authorized activities;
- failures of equipment containing sources which may have security implications; and
- discovery of any unaccounted source.

These reports will enable the Regulatory Authority to keep track of sources and aid in the identification and recovery of lost sources.

5. GUIDELINES FOR SPECIFIC SECURITY MEASURES

As previously discussed, in order to properly design administrative and technical measures focused on security and to assess their appropriateness, the principal party and the Regulatory Authority need a common basis. The design basis threat assessment methodology is recommended as the appropriate tool but other approaches are possible. At least for Security Groups A and B, a basis is needed for the design of the appropriate delay and detection devices. Using the design basis threat instead of prescribing certain measures can provide the opportunity to design the security consistent with the individual prevailing conditions for a certain source or application.

For Security Groups C and D, there is less need for a design basis threat approach and application of existing standards is an appropriate approach. One example of existing standards are the European Norms ENV 1627-1630 [19–22] which define classes of barriers against intrusion attempts. The use of these referenced classes will replace the need to undertake a design basis threat assessment.

The specific administrative and technical security measures provided in this chapter, along with the general administrative measures in Chapter 4, are intended to meet the performance objectives given for each security group. They can, and should, where possible, be modified by an appropriate design basis threat methodology. Whenever it is not possible to implement the specific measures recommended, then other compensatory measures should be employed, wherever possible, that also meet the objectives.

In general, the security measures given in this section are intended to be applied to individual sources. However, the revised Categorization of Radioactive Sources [11] incorporates a method for appropriately categorizing aggregations of sources in one location. Hence if Table 2 is being used as the basis of the security grouping, then further modification is not necessary. Otherwise, the security measures for an aggregation of sources should be appropriately upgraded in accordance with the number, radioactivity and types of sources.

A summary of the recommended measures described below is given in Table 3.

Table 3. Summary of security measures to be considered

<table>
<tr><th>Group A</th><th>Group B</th><th>Group C</th><th>Group D</th></tr>
<tr><td colspan="4">General administrative measures</td></tr>
<tr><td>Daily accounting</td><td>Weekly accounting</td><td>Semi-annual accounting</td><td>Annual accounting</td></tr>
<tr><td colspan="2">Access control to source location allowing timely detection of unauthorized access</td><td>Access control to source location</td><td rowspan="13">No specific provisions.

Routine measures to ensure safe use and protect as an asset</td></tr>
<tr><td colspan="3">Deterrence provided by:</td></tr>
<tr><td>A. Two technical measures separating the source from unauthorized personnel</td><td>B. Two measures (one technical) separating the source from unauthorized personnel</td><td>C. One technical measure separating the source from unauthorized personnel</td></tr>
<tr><td colspan="2">Specific emergency response plan</td><td>Generic emergency response plan</td></tr>
<tr><td colspan="2">Background checks</td><td rowspan="9"></td></tr>
<tr><td colspan="2">Security plan</td></tr>
<tr><td colspan="2">Information security</td></tr>
<tr><td colspan="2">Upgrade security for increased threat</td></tr>
<tr><td colspan="2">Timely detection provided by:</td></tr>
<tr><td>A. Remotely monitored intruder alarm</td><td>B. Local alarm</td></tr>
<tr><td>Timely response to an alarm</td><td></td></tr>
</table>

5.1. Security Group A and B

Security Groups A and B have several commonalities that are addressed in this section.

5.1.1. A and B: Emergency response plans

Specific emergency response procedures should be developed, at least for the A and B security groups, which are appropriate to the magnitude and number of sources. As a minimum, these would normally include notifications in the event of a loss of the source, press release procedures, and initial measures to recover lost or stolen sources. States that are party to the Early Notification Convention [24] are required to follow a notification procedure for *"an international transboundary release that could be of radiological safety significance for another State"*. Loss of control of a Category 1, 2 or 3 source that may cross borders could be included in this notification.

Emergency response procedures should be exercised and evaluated periodically, and a frequency of at least once per year is recommended.

5.1.2. A and B: Background checks

The principal party should ensure that persons engaged in the management of Group A and B sources are trustworthy. The need for confidence in the level of trustworthiness of authorized users of these sources is such that background checks should be made prior to the Regulatory Authority granting the necessary authorization. The nature and depth of background checks is not specified here, but is left to the Regulatory Authority to determine. Others with access to Group A or B sources do not necessarily need background checks as long as they are appropriately escorted or kept under visual surveillance by persons who have undergone background checks.

5.1.3. A and B: Security plans

Sources in Security Groups A and B should have a security plan. The security plan should describe how the security provisions in this document are met for the source(s) under consideration. It should be reviewed at least annually to ensure that it is still current and applicable. Appendix III outlines some of the issues that should be considered in a security plan.

Security systems are only effective if they are fully implemented and if they are periodically tested or evaluated. System evaluations should be performed and documented as part of a quality assurance system.

Whenever there are reasons to believe that any locks or settings may have been compromised they should be changed.

5.1.4. A and B: Information security

For sources in Security Groups A and B, information or documents that can be used to identify specific locations, specific security measures or weaknesses in the principal party's system of management of sources should be controlled and distributed on a need to know basis taking into account the State's regulations on classified documents. This information includes:

- specific locations of sources;
- the facility's security plan and security system associated with the sources;
- temporary or permanent weaknesses in the security system;
- source utilization plans and records;
- proposed date and time of source(s) shipment or transfer;
- emergency response plans and systems.

5.1.5. A and B: Response to an increased threat

The planning for response to an increased threat of malevolent use should take place in close cooperation with the Regulatory Authority and the competent emergency agencies. There should be pre-arranged procedures with law enforcement regarding intelligence information and use of secure communications as well as the reactions to an increased threat.

If a person with responsibility for a Group A or B source becomes aware, or suspects that there is a specific threat targeting a source or source storage location, it is recommended that security be increased in accordance with the threat. The increased security measures should be continued until such time as it is determined that the specific threat is no longer present. The following measures should be considered:

— if the source is in use, return the source to its secure storage location;

— provide a 24-hour guard, or use video observation, or an intrusion alarm;

— ensure that the law enforcement and Regulatory Authorities are made aware of the suspected threat;

— review the security procedures, facility layout, and radiation safety practices with the law enforcement and emergency response personnel;

— make sure that emergency response procedures are current (See Ref. [25]). In particular, ensure that local medical facilities are available where there are personnel trained and equipped to handle radiological emergencies.

5.2. Security Group A

The performance objectives of security measures for sources in Security Group A are to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible.

Ideally, radioactive sources of Group A should be separated from unauthorized personnel by at least two technical measures and have access control; however, during use this may not always be possible. In any situation, the quality of these security measures should be consistent with the design basis threat. Every unauthorized access to the source should be detected in a timely manner.

Sources in Security Group A should be accounted for on a daily basis.

5.2.1. A: Sources in storage

To achieve the defined performance objective, the following provisions could be implemented:

— a locked and fixed container or a device holding the source;
— a locked storage room, separating the container from unauthorized personnel;
— access control to the storage room;
— detection of unauthorized access or removal of the source;
— ability to respond in a timely manner to such detection.

For instance, if a high activity mobile source were in this group, the requirements could be:

— stored in a shielded container, which is locked;
— kept in an enclosed, secured vehicle;

— the vehicle parked inside a locked compound or locked garage;
— the vehicle subject to continuous detection of unauthorized intrusion attempts and there should be the capability to respond to intrusion.

These measures should provide the delay against the defined threat. Depending on the specifics of any threat assessment, additional responses might be required.

5.2.2. A: Sources in use

Security measures for a high-risk source, for example, while in use could be:

— a locked device in a controlled area, separating the container from unauthorized personnel;

— access control to the area;

— the room could be subject to continuous detection of unauthorized intrusion attempt, either by personal surveillance or electronic equipment;

— the building has security guards able to provide a timely response.

These measures should provide the delay against the defined threat. Depending on the assessment of the threat, additional response might be required. If the default assignment is being followed, these measures would be applicable to, for example, a teletherapy source in a hospital.

For a mobile source being used in the field, it is recognized that it might not always be possible to achieve the specified requirements. Therefore, compensatory measures, such as rigorous personal surveillance, must be implemented. In addition, the required security measures should be re-established as soon as possible.

5.2.3. A: Sources in transport

Transport of Security Group A sources should satisfy the performance requirements for security for this group. In addition, they should also satisfy the recommendations that are to be issued in further IAEA publications on security in transport as well as comply with national and international legislation and agreements on security in transport.

As an example of these performance objectives for a Security Group A source, the transport should provide for:

— background checks on trustworthiness of the transport organization and operatives;
— deterence through use of transport packages locked and sealed and in a dedicated transport unit, which is locked;
— timely detection through radio communication between the personnel in the vehicle and a security office or organization;
— response through security trained transport operatives;
— emergency plan developed to deal with emergencies in transit.

Depending on the threat assessment, additional guards or a response force might be required.

However, because of the different modes of transport and complex international issues, further information on security in transport will be developed in forthcoming documents.

5.3. Security Group B

The performance objectives of security measures for sources in Security Group B are to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner.

Ideally, Security Group B sources should be separated from unauthorized access by at least two security measures, with at least one being a technical measure; however, during use this may not always be possible. Access controls should also be established. Every unauthorized access to the source should be detected in a timely manner.

Sources in Security Group B should be accounted for on a weekly basis.

5.3.1. B: Sources in storage

To achieve the defined objective, the following provisions could be implemented:

— a locked and fixed container or a device holding the source;
— a locked room to separate the container from unauthorized access;
— access control to the room;
— ability to detect unauthorized access to, or removal of the source.

5.3.2. B: Sources in use

To achieve the defined objective, the following provisions could be implemented:

— use of the source in a locked room or controlled area;
— continuous surveillance of the source;
— access control to the room or controlled area.

For a mobile source, it is recognized that it might not always be possible to achieve the specified measures. Therefore, the vigilance of an administrative control such as personal surveillance needs to be rigorously maintained. Compensatory measures should also be considered to provide other levels of protection. These could include, for example, establishing a communication link to allow response to incidents, or potential threats. In addition, the required number of measures should be re-established as soon as possible after use.

5.3.3. B: Sources in transport

Transport of Security Group B sources should satisfy the performance requirements for security for this group. In addition, they should also satisfy the recommendations that are to be issued in further IAEA publications on security in transport, as well as comply with national and international legislation and agreements on security in transport.

5.4. Security Group C

The performance objectives of security measures for sources in Security Group C are to deter unauthorized access and to verify the presence of the sources at set intervals.

The principal party should ensure that persons engaged in the management of Group C sources are authorized.

Group C sources should be separated from unauthorized personnel by at least one technical measure. Access control to areas where sources of Group C are present, should also be provided.

A semi-annual accounting of all Security Group C sources should be made.

Generic emergency plans should be sufficient to respond to any incidents with these sources.

5.4.1. C: Sources in storage

To achieve the defined objective, Group C sources could be stored in a locked, fixed container and in a room with control on access.

5.4.2. C: Sources in use

The appropriate control for a Group C source while in use could be to make sure that an authorized person uses the source only in an area that has controlled access, or that the source is in a secure containment in an area where there are personnel able to detect any interference with the source.

5.4.3. C: Sources in transport

Transport of Security Group C sources should satisfy the performance requirements for security for this group. In addition, they should also satisfy the recommendations that are to be issued in further IAEA publications on security in transport, as well as comply with national and international legislation and agreements on security in transport.

5.5. Security Group D

The performance objectives of security measures for sources in Security Group D are to ensure safe use of the source and adequately protect it as an asset, verifying its presence at set intervals.

The personnel in charge of managing sources of Group D should be approved as legitimate authorized personnel. Group D sources should be protected by application of the relevant safety standards as well as appropriate industrial standards. The natural interest of the owner to protect the asset and to ensure safe use and storage is the appropriate basis for the security provided. In addition to these measures, sources should be subject to annual accounting.

Transport should be in accordance with the transport regulations [26].

6. TEMPORARY STORAGE

Following an emergency or the discovery of an orphan source, it may be necessary to temporarily store a radioactive source. Sources may be deemed to be in temporary storage only while the responsible agency or state is actively seeking permanent storage or transfer. Wherever possible, arrangements for the temporary storage of found sources should be pre-planned by the Regulatory Authority. Preferably, sources should be removed from a temporary storage to a designated facility as soon as practicable, with the objective that no source is stored temporarily for greater than 30 days.

As far as possible the source container should be secured in a manner that conforms to the storage recommendations of its group.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Goiânia, IAEA, Vienna (1988).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Tammiku, IAEA, Vienna (1998).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Lilo, IAEA, Vienna (2000).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Istanbul, IAEA, Vienna (2000).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Samut Prakarn, IAEA, Vienna (2002).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nature and Magnitude of the Problem of Spent Radiation Sources, IAEA-TECDOC-620, Vienna (1991).

[7] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, NUCLEAR ENERGY AGENCY OF THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 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).

[8] KROCK, L., DEUSSER, R., Dirty Bomb — Chronology of Events, http://www.pbs.org/wgbh/nova/dirtybomb/chrono.html

[9] WALSH, N.P., Nick Paton Walsh in Moscow, The Guardian, 1 June 2002 (2002).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Draft Revised Code of Conduct on the Safety and Security of Radioactive Sources, IAEA, Vienna (2003).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Revised Categorization of Radiation Sources, IAEA-TECDOC-1344, Vienna (2003).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Physical Protection of Nuclear Materials, INFIRC/274/Rev 1, IAEA, Vienna (1980).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Method for the Development of Emergency Response Preparedness for Nuclear or Radiological Accidents, IAEA-TECDOC-953, Vienna (1997).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Procedures for Assessment and Response during a Radiological Emergency, IAEA-TECDOC-1162, Vienna (2000).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Prevention of the Inadvertent Movement and Illicit Trafficking of Radioactive Materials, IAEA-TECDOC-1311, Vienna (2002).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Detection of Radioactive Materials at Borders, IAEA-TECDOC-1312, Vienna (2002).

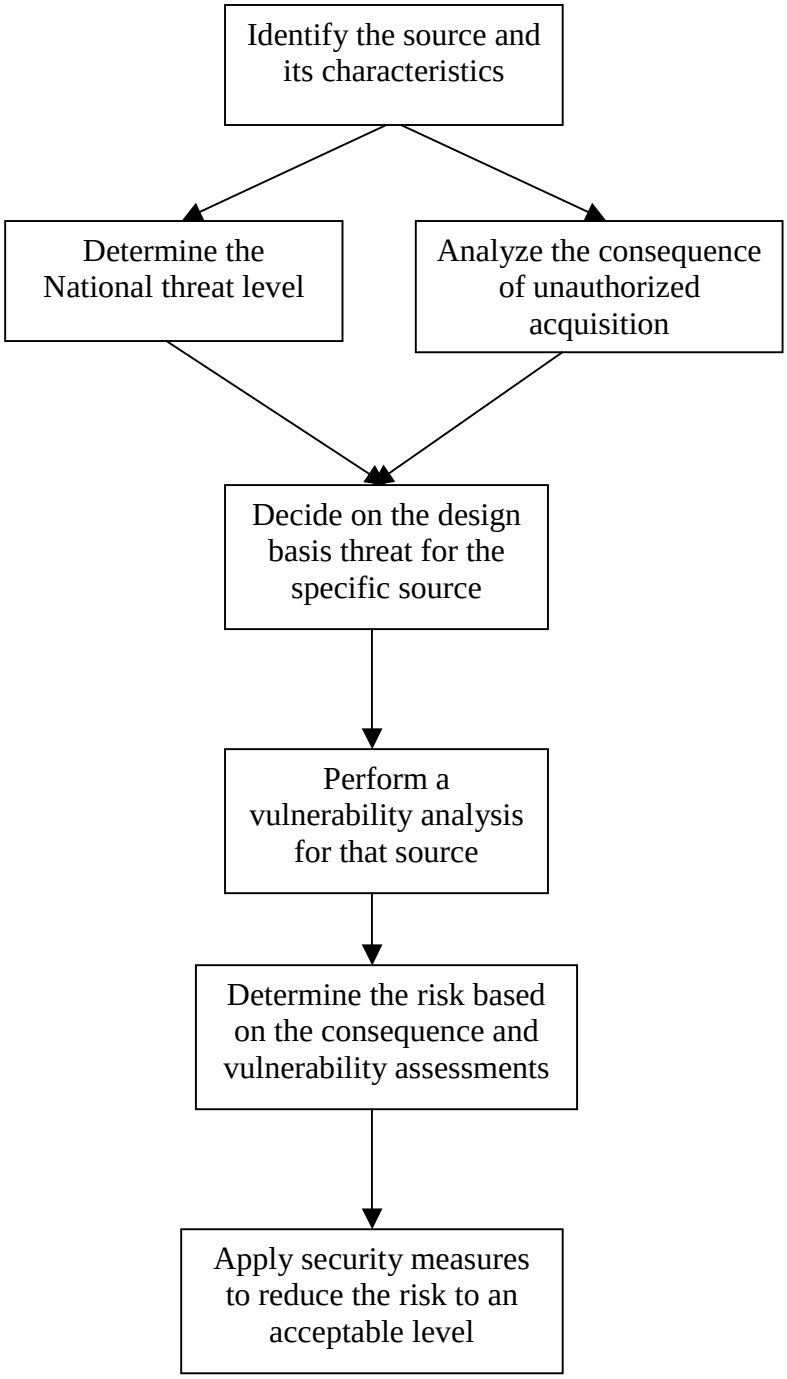
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Response to Events Involving the Inadvertent Movement or Illicit Trafficking of Radioactive Materials, IAEA-TECDOC-1313, Vienna (2002).

[19] UNI ENV 1627/00 Windows, doors, shutters – Burglar resistance – Requirements and classification.

[20] UNI ENV 1628/00 Windows, doors, shutters – Burglar resistance – Test method for the determination of resistance under static loading.

[21] UNI ENV 1629/00 Windows, doors, shutters – Burglar resistance – Test method for the determination of resistance under dynamic loading.
[22] UNI EN 1630/00 Windows, doors, shutters – Burglar resistance – Test method for the determination of resistance to manual burglary attempts.
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety, Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Early Notification of a Nuclear Accident, INFCIRC/335, IAEA, Vienna (1986).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency Safety Requirements, Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, Safety Standards Series No. TS-R-1, IAEA, Vienna (2000).

APPENDIX I. FLOW CHART OF THE DESIGN BASIS THREAT ASSESSMENT PROCESS



APPENDIX II. EXAMPLE OF THE USE OF THE DESIGN BASIS THREAT METHODOLOGY FOR DETERMINATION OF THE SECURITY OF A SOURCE

A city hospital uses ^{137}Cs in high dose-rate brachytherapy. The hospital is in a country where there have been incidents of illicit trafficking of radioactive material. The threat of malicious actions involving sources is therefore considered to be quite high. An analysis was performed of the possible consequences of unauthorized acquisition of these hospital sources.

This analysis showed that the nature and form of the ^{137}Cs sources was such that the radioactive material could be easily dispersed via an explosion or otherwise destroying the source. The advice from intelligence experts did not necessarily conclude that these events would happen in the State but could happen in a neighboring State.

On that basis, the Regulatory Authority determined that the specific design basis threat is the possible acquisition of a brachytherapy source by an insider in the hospital or by people who enter the hospital as patients or contractors.

A vulnerability analysis performed for the particular sources showed that:

— Sources were kept in a locked container in a locked room while not in use.
— Both spent and current sources were in the same room.
— There was no background checking on people who had access to the keys to the room.
— There was no electronic access control or detection in the room.

The risk of successful attempts to acquire the source was therefore considered high, given the national threat, and the Regulatory Authority required additional measures to be put in place. The security level required was considered to be equivalent to the performance requirements in Security Group A in this document.

After discussion between the Regulatory Authority and the hospital management, it was agreed that additional measures were needed:

— introduce background checks on staff having access to the keys to the room;

— remove all spent sources to a national store to reduce the attractiveness of the room to those with malicious intent;

— install radiation detectors at the door and a video camera in the source room. These were relayed to the security guards at the hospital entrance and to the health physics office.

— train the hospital guards in security awareness, in recognizing radiation containers, in the need to protect the sources and in the response procedure for any alarm.

APPENDIX III. SECURITY PLAN CONTENT

A security plan should include everything to evaluate and to understand the security concept being used for the source. The following topics would typically need to be included.

— A description of the source and its use.

— A description of the environment, building and/or facility where the source is used or stored.

— The location of the building or facility relative to areas accessible to the public.

— The objectives of the security plan for the specific application, including:

- the specific concern to be addressed: theft, destruction, or malevolent use;
- the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
- the equipment or premises that will be secured.

— The technical measures to be used, including:

- the measures to secure, provide surveillance, detect, delay, respond and communicate; and
- the design features to evaluate the quality of the measures against the assumed threat.

— The administrative measures to be used, including:

- the roles and responsibilities of the various people and groups;
- routine and non-routine operations;
- maintenance;
- determination of the trustworthiness of personnel;
- the application of information security;
- methods for access authorization;
- emergency plans;
- training.

— References to existing regulations or standards.

CONTRIBUTORS TO DRAFTING AND REVIEW

Abs Eksalam, A.	Nuclear Power Plants Authority, Egypt
Cameron, R.F.	International Atomic Energy Agency
Colgan, P.	Australian Radiation Protection and Nuclear Safety Agency, Australia
Cox, C.	Nuclear Regulatory Commission, United States of America
Crick, M.	International Atomic Energy Agency
Dodd, B.	International Atomic Energy Agency
Goevelinger, N.L.	International Atomic Energy Agency
Hagemann, A.	International Atomic Energy Agency
Legoux, P.M.C.	International Atomic Energy Agency
Liu, S.	China Institute of Atomic Energy, China
Molnar, K.	Hungarian Atomic Energy Authority, Hungary
Nandukumar, A.N.	Atomic Energy Regulatory Board, India
Orfi, S.D.	Pakistan Institute of Nuclear Science and Technology, Pakistan
Pellet, S.	National Research Institute for Radiobiology and Radiohygiene, Hungary
Peto, A.	Hungarian Atomic Energy Authority, Hungary
Piotukh, O.	Ministry for Emergencies of the Republic of Belarus, Belarus
Pope, R.	International Atomic Energy Agency
Reber, E.H.	International Atomic Energy Agency
Soo Hoo, M.S.	International Atomic Energy Agency
Sroka, M.	State Office for Nuclear Safety
Stålnacke, C.	Swedish Radiation Protection Authority, Sweden
Torres, G.	Permanent Mission of Chile, Chile
Viglasky, T.	Canadian Nuclear Safety Commission, Canada
Weedon, C.	The Environment Agency, United Kingdom
Wheatley, J.S.	International Atomic Energy Agency
Wrixon, A.D.	International Atomic Energy Agency
Xu, P.	China Atomic Energy Authority, China