SECURITY OF RADIOACTIVE
MATERIAL IN USE AND STORAGE
AND OF ASSOCIATED FACILITIES

(REVISION OF NUCLEAR SECURITY SERIES NO. 11)

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX
FOREWORD

(standard foreword to be inserted)
## CONTENTS

1. INTRODUCTION .............................................................................................................................. 5
   1.1. Background ........................................................................................................................... 5
   1.2. Objective ............................................................................................................................. 5
   1.3. Scope ................................................................................................................................... 6
   1.4. Structure .............................................................................................................................. 7

2. OBJECTIVES OF A STATE’S NUCLEAR SECURITY REGIME FOR RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES .............................................. 8
   2.1. Overall Objective ................................................................................................................ 8
   2.2. Means of Achieving the Objectives .................................................................................... 9

3. ELEMENTS OF A STATE’S NUCLEAR SECURITY REGIME FOR RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES ........................................ 9
   3.1. State Responsibility........................................................................................................... 10
   3.2. Assignment of Nuclear Security Responsibilities ............................................................. 10
   3.3. Legislative and Regulatory Framework ............................................................................ 12
       3.3.1. State ....................................................................................................................... 12
       3.3.2. Regulatory body .................................................................................................... 20
       3.3.3. Operator ................................................................................................................ 22
   3.4. International Cooperation and Assistance ......................................................................... 24
   3.5. Identification and Assessment of Threats ......................................................................... 25
       3.5.1. National threat assessment .................................................................................... 25
       3.5.2. Design basis threat or alternative threat statement (DBT or ATS) ....................... 28
       3.5.3. Insider threats ....................................................................................................... 29
       3.5.4. Increased threat ..................................................................................................... 30
       3.5.5. Protection against threats beyond the DBT or ATS ............................................... 30
       3.5.6. Evaluation methods ............................................................................................... 30
   3.6. Risk Based Nuclear Security Systems and Measures ....................................................... 31
       3.6.1. Risk management ................................................................................................. 31
       3.6.2. Interfaces with the safety system .......................................................................... 35
   3.7. Sustaining the Nuclear Security Regime ........................................................................... 39
       3.7.1. National level ........................................................................................................ 39
       3.7.2. Operational level ................................................................................................... 40
   3.8. Planning and Preparedness for and Response to Nuclear Security Events ....................... 41
   3.9. Import and Export of Radioactive Material ....................................................................... 42
   3.10. Detection of Nuclear Security Events ............................................................................. 43
4. SECURITY CONCEPTS ................................................................................................................. 44
   4.1. Purpose of a security system ............................................................................................. 44
   4.2. Security functions ............................................................................................................. 44
   4.3. Design and evaluation of security systems ....................................................................... 45
5. ESTABLISHING A REGULATORY PROGRAMME FOR THE SECURITY OF RADIOACTIVE MATERIAL .............................................................................................................. 46
   5.1. Step 1: Establish Graded Security Levels With Corresponding Goals and Objectives .... 47
   5.2. Step 2: Determine the Security Level Applicable to Radioactive Material: Security-Based Categorization ............................................................................................................................... 49
      5.2.1. Categorization ....................................................................................................... 49
      5.2.2. Assigning security levels ...................................................................................... 55
      5.2.3. Additional considerations for adjusting security levels ........................................ 56
   5.3. Step 3: Implement a Regulatory Approach ....................................................................... 59
      5.3.1. What is the operator required to protect? .............................................................. 60
      5.3.2. What is the operator required to protect against? .................................................. 60
      5.3.3. What degree of protection is adequate? ................................................................ 61
      5.3.4. What are the security measures the operator is required to implement? ............... 61
      5.3.5. What are the security management measures the operator is required to implement? ............................................................................................................................ 62
6. RECOMMENDATIONS ON THE CONTENT OF REGULATIONS ........................................... 62
   6.1. Prescriptive approach ........................................................................................................ 62
      6.1.1. Introduction for Security Level A measures ......................................................... 63
      6.1.2. Introduction for Security Level B measures ......................................................... 65
      6.1.3. Introduction for Security Level C measures ......................................................... 69
      6.1.4. Introduction for security management measures .................................................. 71
   6.2. Performance Based Approach ........................................................................................... 77
   6.3. Combined approach ........................................................................................................ 78

APPENDIX I. DESCRIPTION OF SECURITY MEASURES ................................................................................. 79
APPENDIX II. TOPICS TO BE ADDRESSED IN AN OPERATOR’S SECURITY PLAN .......... 83
APPENDIX III. DESCRIPTION OF A VULNERABILITY ASSESSMENT ......................................................... 86
REFERENCES ..................................................................................................................................... 88
GLOSSARY ......................................................................................................................................... 91
1. INTRODUCTION

1.1. BACKGROUND

The IAEA Nuclear Security Series provides guidance for States to assist them in implementing new nuclear security regimes, or in evaluating and if necessary strengthening existing nuclear security regimes. The series also serves as guidance for Member States in carrying out their efforts with respect to binding and non-binding international instruments.

The Nuclear Security Fundamentals provide the objective and essential elements for the entire nuclear security regime [1]. The Nuclear Security Recommendations indicate what a nuclear security regime should address for:

(a) Physical Protection of Nuclear Material and Nuclear Facilities [2]
(b) Radioactive Material and Associated Facilities [3]
(c) Nuclear and Other Radioactive Material out of Regulatory Control [4]

This publication is the lead Implementing Guide for the Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3].

This Implementing Guide is a revision of the Implementing Guide Security of Radioactive Sources published in 2009 as Nuclear Security Series No. 11. This revision was undertaken to better align this publication with the relevant Recommendations [3] (which were prepared after publication of the original Implementing Guide); to expand the scope to include not only radioactive sources as defined in the Code of Conduct on the Safety and Security of Radioactive Sources [5], but also to address all radioactive material and associated facilities as defined in Ref. [3]; to cross-reference other relevant guidance published since 2009; and to selectively add further detail on certain topics based on the experience of the IAEA and Member States in using the original Implementing Guide.

1.2. OBJECTIVE

The objective of this publication is to provide guidance to Member States and their competent authorities (primarily regulatory bodies) on how to establish or improve, implement, maintain, and sustain their nuclear security regime for radioactive material, associated facilities, and associated activities, with particular emphasis on the development of regulatory requirements. The State’s nuclear security regime for radioactive material and associated facilities and activities is an essential component of the State’s overall nuclear security regime.

The present publication will assist States to implement a comprehensive nuclear security regime, including any obligations and commitments they might have with respect to international instruments related to the security of radioactive material, associated facilities and associated activities such as the
Conduct on the Safety and Security of Radioactive Sources [5] and its supplementary Guidance on the
Import and Export of Radioactive Sources [7].

In some sections in this publication the distinction between the State and its competent authorities has
not been precisely defined. This ambiguity recognizes the differences among Member States with
respect to the assignment of responsibilities among a State’s competent authorities. Nonetheless, a
State should be precise and complete in assigning and documenting nuclear security responsibilities.

1.3. SCOPE

This publication is a revised version of, and supersedes, the Implementing Guide Security of
Radioactive Sources published in 2009 as Nuclear Security Series No. 11.

This publication applies to the security of radioactive material, associated facilities and associated
activities (other than transport) for the prevention of acts or attempts of unauthorized removal or
sabotage intended or likely to cause harmful radiological consequences. Such radioactive material
includes radioactive sources and unsealed radioactive material including radioactive material over
which regulatory control has been gained or regained. If possible and where appropriate, States should
also consider the application of this guidance to radioactive waste. The term ‘radioactive material’ is
used throughout this guidance, but its application to all radioactive material beyond radioactive
sources will depend on national context and priorities.

This publication addresses the security of radioactive material throughout its life cycle: manufacture,
supply, receipt, possession, storage, use, transfer, import, export, maintenance, recycling and disposal.
In this publication, security refers to both security systems and security management measures.

Other Implementing Guides and Technical Guidance provide guidance that is relevant to
implementation of the Recommendations [3]. These include:

(a) Regulations and Associated Administrative Measures [8];

(b) Sustaining a Nuclear Security Regime [9];

(c) Others as considered necessary.

In relation to these publications, this Implementing Guide summarizes the key guidance as it relates to
the security of radioactive material and associated facilities and then refers to the most relevant
provisions of these other documents.

This publication does not cover preparedness and response to a nuclear or radiological emergency
triggered by a nuclear security event, which are addressed in Refs [10] and [11].
The security of radioactive material in transport is addressed in Ref. [12]. Section 3 repeats some provisions related to transport from Ref. [3], but references to shippers and/or carriers have been deleted because transport is not within the scope of this Implementing Guide.

Radioactive material also includes nuclear material. However, this publication applies only to the protection of nuclear material against unauthorized removal for potential subsequent off-site exposure or dispersal leading to harmful radiological consequences.

This publication does not apply to the physical protection of nuclear material against unauthorized removal for use in a nuclear explosive device or to the physical protection of nuclear facilities against sabotage. These topics are addressed in Ref. [2] and its supporting Implementing Guide [13]. When a facility contains nuclear material and other radioactive material, the protection requirements for both should be considered and implemented in a consistent and non-conflicting manner in order to achieve an adequate level of security.

Many States have applied the guidance in the original Implementing Guide in establishing regulatory requirements for the security of radioactive sources. This revised Implementing Guide should not be read to imply that such States need to amend their regulations to be consistent with the revised guidance. However, they may choose to expand the scope of their regulatory programmes or make modifications over time, consistent with national priorities and changing circumstances, such as threat.

This publication assumes that the State has established and implemented a legislative and regulatory framework for the control and safety of radioactive material and associated facilities, including enabling legislation, a regulatory body, a national register (inventory) of radioactive material, an authorization process, regulatory requirements for safety, and provision for inspection and enforcement. In this publication, safety is also intended to cover radiation protection. Such elements are addressed more completely in Refs [14] to [17].

1.4. STRUCTURE

The remaining structure of this publication is as follows. Section 2 sets out the objectives of the State’s nuclear security regime for radioactive material, associated facilities and associated activities. Section 3 provides guidance for the State and its competent authorities regarding elements of the nuclear security regime. Section 4 contains general information on security functions and security concepts. Section 5 provides guidance regarding the development of regulatory requirements for the security of radioactive material. Section 6 gives detailed guidance on establishing regulatory requirements using the prescriptive approach and more general guidance on the performance-based and combined approaches. Three Appendices provide: a description of security measures discussed in
2. OBJECTIVES OF A STATE’S NUCLEAR SECURITY REGIME FOR RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES

2.1. OVERALL OBJECTIVE

The overall objective of a State’s nuclear security regime is to protect persons, property, society, and the environment from malicious acts involving nuclear material or other radioactive material that could cause harmful radiological consequences.

Such malicious acts and potential consequences could include:

(a) Unauthorized removal of radioactive material for:

- use in a radiological dispersal device (RDD), the spread of radioactive material using conventional explosives, or by other means, for the purpose of, inter alia, causing health effects, or contaminating ground, buildings and infrastructure, leading to denial of access to these areas, or denial of service from the infrastructure;

- use in a radiation exposure device (RED), the use of radioactive material in a device designed to intentionally expose members of the public to radiation;

- the deliberate placement of unshielded radioactive material in a public area; or

- the deliberate placement of radioactive material in food or water to cause radiation doses or poisoning through ingestion.

(b) Sabotage of radioactive material in place in order to achieve one or more of the same purposes;

The more specific objectives of a nuclear security regime for radioactive material, associated facilities and associated activities should include:

(a) Protection against unauthorized removal of radioactive material used in associated facilities and in associated activities;

(b) Protection against sabotage of radioactive material, associated facilities and associated activities;
(c) Ensuring the implementation of rapid and comprehensive measures to locate, recover, as appropriate, radioactive material which is lost, missing or stolen and to re-establish regulatory control. [3]

Insofar as they apply to radioactive material which is also nuclear material, the first and second objectives are addressed in this Implementing Guide only with respect to protection of such nuclear material against unauthorized removal for potential subsequent off-site exposure or dispersal leading to harmful radiological consequences. Protection of nuclear material against unauthorized removal for use in a nuclear explosive device and protection of nuclear facilities against sabotage are addressed in [2, 13].

The third objective is mainly related to radioactive material out of regulatory control, which is addressed in Ref. [4] and its supporting Implementing Guides.

2.2. MEANS OF ACHIEVING THE OBJECTIVES

These objectives are achieved through the establishment of a nuclear security regime which includes security measures to deter, detect, delay and respond to a potential malicious act, and to provide for the security management of radioactive material and associated facilities and associated activities.

These security measures should be based on a graded approach, taking into account the principles of risk management, including such considerations as the level of threat and the relative attractiveness of the radioactive material for a malicious act (based on such factors as quantity, physical and chemical properties, mobility, availability and accessibility). Security measures should be adapted depending on whether the radioactive material concerned is sealed, unsealed, disused, or waste. This graded approach ensures that the highest consequence material receives the greatest degree of security.

Security measures should also take into account the concept of defence in depth: the use of several layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by an adversary.

Recognizing the societal benefits of using radioactive material, the nuclear security regime should strive to achieve a balance between managing radioactive material securely without unduly limiting the conduct of those beneficial activities.

3. ELEMENTS OF A STATE’S NUCLEAR SECURITY REGIME FOR RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES

This section provides guidance on the principles, concepts and approaches for implementing the elements of a State’s nuclear security regime for radioactive material, associated facilities and associated activities identified in Ref. [3].
3.1. STATE RESPONSIBILITY

“The responsibility for the establishment, implementation and maintenance of a nuclear security regime within a State rests entirely with that State.” (Ref. [3], para. 3.1)

To meet this responsibility, the State should take the appropriate steps to ensure that the nuclear security regime securely protects radioactive material within the State’s territory, or under its jurisdiction or control. This regime should place the prime responsibility on the operator for implementing and maintaining security measures for radioactive material, associated facilities and associated activities.

3.2. ASSIGNMENT OF NUCLEAR SECURITY RESPONSIBILITIES

“The State should clearly define and assign nuclear security responsibilities to competent authorities, noting that they may include regulatory bodies, law enforcement, customs and border control, intelligence and security agencies, health agencies, etc.” (Ref. [3], para. 3.2)

To ensure that operators meet their prime responsibility for security, the State should clearly define and assign nuclear security responsibilities to one or more competent authorities and confer upon each the powers necessary to perform their assigned functions. Table 1 depicts a typical assignment of nuclear security responsibilities to competent authorities. A State’s actual assignment of such responsibilities may vary depending on national law, practice and circumstances. However, each responsibility indicated in the second column of Table 1 should be assigned to at least one competent authority.
<table>
<thead>
<tr>
<th>Competent Authority</th>
<th>Nuclear Security Responsibilities and Powers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory body</td>
<td>Establish a system of regulatory control over radioactive material, associated facilities and associated activities that places the primary responsibility for nuclear security on authorized persons (licensees)</td>
</tr>
<tr>
<td></td>
<td>Establish a system of security-based categorization</td>
</tr>
<tr>
<td></td>
<td>Develop and maintain national register of radioactive material</td>
</tr>
<tr>
<td></td>
<td>Participate in national threat assessment</td>
</tr>
<tr>
<td></td>
<td>Develop and apply design basis threat, alternative threat statement, or other defined threat for purposes of regulation for security</td>
</tr>
<tr>
<td></td>
<td>Implement authorization (licensing) process, including review and assessment of security systems and security management measures</td>
</tr>
<tr>
<td></td>
<td>Establish regulatory requirements and provide guidelines for security, including requirements for information protection</td>
</tr>
<tr>
<td></td>
<td>Manage the safety-security interface</td>
</tr>
<tr>
<td></td>
<td>Conduct security inspections</td>
</tr>
<tr>
<td></td>
<td>Take enforcement action for non-compliance</td>
</tr>
<tr>
<td></td>
<td>Participate in regional and international databases and other cooperative activities</td>
</tr>
<tr>
<td></td>
<td>Encourage and promote a robust nuclear security culture</td>
</tr>
<tr>
<td></td>
<td>Participate in planning and preparedness for and response to nuclear security events, including participation in exercises</td>
</tr>
<tr>
<td></td>
<td>Administer procedures for authorizing and controlling the import and export of radioactive material</td>
</tr>
<tr>
<td></td>
<td>Notify operators concerning specific or increased threat</td>
</tr>
<tr>
<td></td>
<td>Review and assess the design of security system (in the authorization process)</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>Provide response to interrupt malicious acts (unauthorized access, unauthorized removal, sabotage)</td>
</tr>
<tr>
<td></td>
<td>Participate in planning and preparedness for and response to nuclear security events, including participation in exercises</td>
</tr>
<tr>
<td></td>
<td>Participate in national threat assessment</td>
</tr>
<tr>
<td></td>
<td>Identify specific or increased threats</td>
</tr>
<tr>
<td></td>
<td>Conduct background checks for purposes of trustworthiness verification</td>
</tr>
<tr>
<td></td>
<td>Detect and investigate nuclear security events</td>
</tr>
<tr>
<td>Customs and border control</td>
<td>Participate in national threat assessment</td>
</tr>
<tr>
<td></td>
<td>Identify specific or increased threats</td>
</tr>
<tr>
<td></td>
<td>Control and detect non-compliance with respect to imports or exports</td>
</tr>
<tr>
<td></td>
<td>Communicate with regulatory body with respect to national inventory of radioactive material</td>
</tr>
</tbody>
</table>
Competent Authority | Nuclear Security Responsibilities and Powers
--- | ---
Intelligence and security agencies | Direct national threat assessment
 | Identify specific or increased threats
National emergency response agency | Coordinate planning and preparedness for and response to nuclear security events
Civil defence, health and environment agencies | Participate in planning and preparedness for and response to nuclear security events
Ministry of justice and prosecuting authorities | Impose sanctions against perpetrators of malicious acts
Ministry of foreign affairs | Engage in regional and international cooperation

“Provision should be made for appropriate integration and coordination of responsibilities within the State’s nuclear security regime. Clear lines of responsibility and communication should be established and recorded between the competent authorities.

“The State should ensure effective overall cooperation and relevant information sharing between the competent authorities. This should include sharing of relevant information (such as information about the threat to be protected against and other useful intelligence) in accordance with national regulations.” (Ref. [3], paras 3.2–3.3)

The State may consider establishing a coordinating body that includes competent authorities with assigned nuclear security responsibilities and that meets regularly for the purpose of ensuring adequate integration, communication, and coordination. One of the competent authorities should be assigned as the lead of this coordinating body. In addition, the State may consider promoting the use of such instruments as memoranda of understanding (MOUs), inter-agency agreements, and the like as a means of facilitating cooperation and information sharing among competent authorities.

3.3. LEGISLATIVE AND REGULATORY FRAMEWORK

3.3.1. State

“The State should establish, implement, and maintain an effective national legislative and regulatory framework to regulate the nuclear security of radioactive material, associated facilities and associated activities, which:

- Takes into account the risk of malicious acts involving radioactive material that could cause unacceptable radiological consequences;
• Defines the radioactive material, associated facilities and associated activities which are subject to the nuclear security regime in terms of nuclides and quantities of radioactive material present;

• Prescribes and assigns governmental responsibilities to relevant entities including an independent regulatory body;

• Places the prime responsibility on the operator, for implementing and maintaining security measures for radioactive material;

• Establishes the authorization process for radioactive material, associated facilities and associated activities. As appropriate, the authorization process concerning the security of radioactive material could be integrated within one defined for safety or radiation protection;

• Establishes the inspection process for security requirements;

• Establishes the enforcement process for the failure to comply with security requirements established under legislative and regulatory framework;

• Establishes sanctions against the unauthorized removal of radioactive material and sabotage of associated facilities and associated activities;

• Takes into account the interface between security and safety of radioactive material.” (Ref. [3], para. 3.4)

As indicated in Ref [8], a State’s legislative and regulatory framework for nuclear security generally comprises several levels, including primary legislation (enactments by a parliament or other legislature), regulations, agreements among competent authorities, and associated administrative measures (guidance documents, procedures, administrative manuals, forms, and the like). Table 2 depicts the elements of an illustrative legislative and regulatory framework for radioactive material, associated facilities and associated activities at each of these levels. Depending on the State’s national legal structure, the level at which these elements are addressed may vary.

<table>
<thead>
<tr>
<th>TABLE 2. ILLUSTRATIVE ELEMENTS OF A LEGISLATIVE AND REGULATORY FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
</tr>
<tr>
<td>Primary Legislation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Level</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>Regulations</td>
</tr>
<tr>
<td>Agreements</td>
</tr>
<tr>
<td>Associated Administrative Measures</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The examples in this table are illustrative. The detailed contents of a State’s legislative and regulatory framework should reflect its national practice and needs. The examples provide a starting point for establishing or strengthening such a framework.

The legislative and regulatory framework for the security of radioactive material should take into account the existence of the legislative and regulatory framework for safety and radiation protection.

Often, a single regulatory body is responsible for authorization and oversight, for both safety and security, in which case authorization may be conducted in a single, integrated process. If the same regulatory body is not responsible for both safety and security, there should be regular, systematic cooperation and information sharing between regulatory bodies for safety and security. In all cases, the interfaces between safety and security requirements should be appropriately managed.
“The State should take appropriate steps within the legislative and regulatory framework to establish and ensure the proper implementation of its nuclear security regime throughout the life cycle of the radioactive material.” (Ref. [3], para. 3.5)

Radioactive material should be subject to an authorization requirement and associated regulation, wherever it is present, throughout all stages of its lifecycle.

In many States, there will be a single authorization for the given radioactive material, addressing both safety and security. In order to obtain the authorization, the applicant should be required to demonstrate that it will meet applicable safety and security requirements, both of which are generally established by regulation. Once the applicant has made this demonstration and the regulatory body has issued the authorization, compliance with these requirements are generally made a condition of the authorization. In some States, an authorization for safety purposes is already in place when the regulatory body establishes security requirements. In such cases, the regulatory body should ensure that these security requirements are mandatory for existing authorization holders, for example through amendment of the existing authorization or by including in the security requirements a specific provision that they are mandatory for existing authorization holders.

“The State should designate one or more competent authorities, including a regulatory body, for the establishment, implementation and maintenance of a nuclear security regime, which have a clearly defined legal status and independence from the operator and which have the legal authority to enable them to perform their responsibilities and functions effectively.” (Ref. [3], para. 3.6)

The State may choose to designate a single regulatory body with responsibility for authorization, inspection and enforcement with respect to the security of all radioactive material, or designate more than one such body with shared responsibilities and functions depending on the use of radioactive material – for example, one regulatory body with jurisdiction over medical uses of radioactive material and another with jurisdiction over industrial and other uses. In such cases, the boundary between the respective jurisdictions should be clearly drawn, and the regulatory approaches should be consistent and compatible.

In all cases, the regulatory body or bodies should be independent from the operators which they regulate. Practices that promote such independence include:

(a) Functional separation of the regulatory body from entities having responsibilities or interests that could unduly influence its decision making;

(b) Ability of the regulatory body to perform its functions without undue influences that might compromise security, such as pressure associated with changing political circumstances or economic conditions, or pressures from government departments or from other organizations;
Refraining from assignment of responsibilities to the regulatory body that might compromise or conflict with its discharging of its responsibility for regulating the security of facilities and activities;

Prohibition of direct or indirect interest of the staff of the regulatory body in facilities and activities or authorized parties beyond the interest necessary for regulatory purposes;

In the event that a department or agency of government is itself an authorized party that operates a regulated facility or facilities or conducts regulated activities, separation and effective independence of the regulatory body from the operating organization;

When new staff members are recruited from operating organizations, emphasis of the independence of the regulatory body in their orientation and training.

“The State should ensure that the regulatory body and other competent authorities are adequately provided with the necessary authority, competence and financial and human resources to fulfil their assigned nuclear security responsibilities.” (Ref. [3], para. 3.7)

Such authority, competence and financial and human resources of the regulatory body should include:

(a) Legal authority for establishment of regulations, authorization, inspection and enforcement with respect to the security of radioactive material;

(b) Personnel with the competence to effectively develop security regulations, assess operators’ demonstration of compliance with security requirements, conduct security inspections and identify corrective actions, and recommend or take enforcement action as a result of non-compliance; and

(c) Sufficient, regular, stable budgets to develop and maintain the foregoing competencies.

If regulatory body safety or radiation protection personnel are assigned to perform security functions, they should receive appropriate training before assuming such responsibilities.

“The State should establish requirements in accordance with national practices to ensure appropriate protection of specific or detailed information, which could compromise the security of radioactive material, associated facilities and associated activities if the information were disclosed.” (Ref. [3], para. 3.8)

Sensitive information is information whose unauthorized disclosure, i.e. compromise (or modification, alteration, destruction or denial of use) could compromise security and otherwise assist in a malicious act.

States should designate the types of sensitive information that are of security concern and should be protected. These may include:
(a) Details of the security measures in place for radioactive material, associated facilities, or associated activities, including information on guard and response forces;

(b) Information relating to the quantity, form, and location of radioactive material, including radioactive material accounting information;

(c) Details of all computer systems including communication systems that process/handle/store and/or transmit information that is directly or indirectly important to security;

(d) Response plans;

(b) Personal information about employees, vendors and contractors;

(f) Threat assessments and information;

(g) Details of sensitive technology;

(h) Details of vulnerabilities or weaknesses that relate to the above topics;

(i) Historical information on any of the above topics.

Information security refers to the system, programme, or set of rules in place to ensure the confidentiality, integrity, authenticity, authorization, and availability of sensitive information in any form. It includes at a minimum the following:

(a) Security of information in physical form (e.g. paper, electronic media, parts, equipment);

(b) Security of computer systems, sometimes referred to as computer security, both those that contain sensitive information and those that control security and operational systems;

(c) Security of communication systems and networks;

(d) Security of intangible information, e.g., knowledge.

Information security should be considered and applied in the context of the overall security framework. It is closely interdependent with other security domains such as physical security and personnel security. Gaps or shortfalls in any of the security domains can impact security in the others, so it is essential to use a comprehensive approach considering all domains together.

To support the security of information, a national framework is necessary to ensure proper handling of sensitive information across all facilities, sites and organizations (government or private). It should include establishing: responsibilities of the State, a legal and regulatory framework, national guidance, security policies, and classification of information according to its sensitivity. This framework should be a national system, not one specific to the radioactive material industry or devised by a single facility, and based on a risk informed approach.
In many instances, States already maintain a classification system but it may not address nuclear security specific information. In such cases, the State should extend the scope of its classification system to nuclear security information. This classification system should establish policies, procedures and systems necessary to ensure that sensitive information is properly marked, controlled and protected both by operators and by the competent authorities themselves.

Each organization and facility which handles sensitive information should then compile its own dedicated security policy based on that of the competent authorities where applicable. This policy should be communicated throughout the organization in a form that is relevant, accessible and understandable to the intended users.

Access to sensitive information should be provided only to authorized individuals who have an operational need to know the information and who have been deemed trustworthy through a background check.

Individuals who possess sensitive information should be required to protect the information from unauthorized disclosure and report any actual or suspected unauthorized release, compromise or failure to protect sensitive information.

Ref. [18] provides more comprehensive guidance on information security requirements.

“The State should ensure that measures, consistent with national practices, are in place to ensure the trustworthiness of persons with authorized access to sensitive information or, as applicable, to radioactive material, associated facilities and associated activities.” (Ref. [3], para. 3.9)

The State should require the regulatory body to verify the trustworthiness of its staff that have access to sensitive information. In addition, the State should authorize and direct the regulatory body to require operators to establish policies and procedures to confirm the trustworthiness of individuals authorized for unescorted access to radioactive material or access to sensitive information through a background check. The regulatory body should ensure the availability of arrangements to enable operators to implement this requirement, such as referral to law enforcement or other external agencies for conduct of the review. In some States, this referral process may require facilitation by the regulatory body. The regulatory body or other competent authority should require that the results of trustworthiness verifications are appropriately protected as sensitive information.

States and regulatory bodies also have various roles to support the operator’s ability to fulfil their responsibility. For example, laws or regulations may be needed to define minimum requirements, standards and scope for background checks, or to establish penalties for misrepresenting material facts during the background check. States and regulatory bodies should also establish a framework that provides the capability to search criminal and counter terrorism databases as part of the background
check. The details of these arrangements will vary depending upon the State’s legislative and regulatory framework.

“The State should establish, develop and maintain a national register of radioactive material over thresholds defined by the State. This national register should, as a minimum, include Category 1 and 2 radioactive sealed sources, as described in the Code of Conduct on the Safety and Security of Radioactive Sources. Other radioactive material could, as appropriate, be included in this register.”

(Ref. [3], para. 3.10)

The State should authorize and require the regulatory body or other competent authority to establish, develop, and maintain a national register. The register should, at a minimum, include all Category 1 and 2 radioactive sources, but may also include any other radioactive material which the State has determined is important for security. The register may already have been established for safety purposes. Examples of information which could be included for each entry in the register are the following, as applicable:

(a) Authorized person (licensee), and associated contact information;
(b) Radioisotope(s);
(c) Physical/chemical form;
(d) Activity level and date of measurement;
(e) Category/security level;
(f) Unique identifier of the radioactive source;
(g) Manufacturer source certificate
(h) Location;
(i) Type of radioactive material (sealed source, unsealed material, etc.);
(j) Practice or use;
(k) Device in which the radioactive material is housed, including model number;
(l) Device serial number;
(m) Manufacturer of the device and associated contact information;
(n) Manufacturer and supplier of the radioactive material and associated contact information;
(o) Date of supply of radioactive material
(p) Intended design lifetime of the radioactive material and/or device;
(q) Photograph of the device and/or radioactive material;
Each operator should be required to maintain an inventory which includes, at a minimum, all Category 1 and 2 radioactive sources. Annually, or at another more frequent interval specified by the regulatory body, the operator should be required to verify that the inventory is complete and accurate in all respects, and adjust the inventory to reflect any discrepancies identified. The operator should be required to report these inventory results to the regulatory body or other competent authority, as applicable, for inclusion in the national registry of radioactive material. The operator should also be required to report receipts and transfers of radioactive material, either prospectively or within a specified time period.

3.3.2. Regulatory body

“The regulatory body should implement the legislative and regulatory framework and authorize activities only when they comply with its nuclear security regulations. Where it is required, the security plan can be used by the regulatory body in its determination for issuance of an authorization.” (Ref. [3], para. 3.11)

The regulatory body should define the requirements for authorization in relation to the security of radioactive material, and establish a process for review and approval (or denial) of applications for new authorizations and renewals or amendments to existing authorizations. As previously noted, the authorization in relation to security may be part of the authorization in relation to safety or it may be a separate authorization. An authorization that includes both safety and security is generally preferable, both because such an authorization more readily address the safety-security interface and because a single authorization is more effectively administered by the regulatory body and implemented by the operator.

Radioactive material should be subject to authorization throughout its life cycle. All authorizations may be subject to amendment, renewal, revocation, or suspension as determined to be necessary by the regulatory body in conformance with established procedures and criteria.

Each authorization should include:

(a) A requirement of compliance with the relevant legislation and regulations;
(b) Specific activity or activities authorized; and
(c) Any constraints regarding the activities, i.e. requirements, conditions, location or time limits.

Assessment of each application should be supported by a review of the security measures proposed by the applicant. Should any deficiencies be identified, the regulatory body should ensure that these
deficiencies are corrected and verified to be acceptable in accordance with established criteria and procedures.

When required by the regulatory body based on a graded approach, the security plan should be one of the documents that are required to be submitted by the applicant to the regulatory body as part of the authorization process. Compliance with an approved security plan should be a condition of the authorization once it is granted. The authorization itself should be an enforceable instrument authorizing an activity or activities subject to compliance with authorization conditions and applicable legislation and regulations.

“The regulatory body should verify continued compliance with nuclear security regulations and relevant authorization conditions, notably through periodic inspections and ensuring that corrective action is taken, when needed. Inspections of security measures implemented by an operator could be performed together with inspections for verifying compliance with other regulatory requirements, such as radiation protection and safety. The security plan could be referred to by the regulatory body for these activities.” (Ref. [3], para. 3.12)

The regulatory body should develop and implement a programme of security inspections of facilities and activities to verify that the operator is in compliance with applicable regulatory requirements and with the conditions specified in the authorization. This programme should specify the types of regulatory inspection (including scheduled inspections and unannounced inspections). The frequency and depth of inspections should be commensurate with the security risks associated with the facility or activity, in accordance with a graded approach. Security could be addressed as part of safety and radiation protection inspections, provided that the inspectors are appropriately trained and qualified in security.

The regulatory body should record the results of inspections and should take appropriate follow-on action (including enforcement actions as necessary). Results of inspections should be used as feedback information for the regulatory process and should be provided to the operator. Inspection results which are security-sensitive should be handled as such. Provision should be made for access by regulatory inspectors to any facility or activity at any time, within the constraints of ensuring operational safety and security at all times and other constraints associated with the potential for harmful radiological consequences.

The regulatory body should establish and implement an enforcement policy within the legal framework for responding to non-compliance by operators with regulatory requirements or with any conditions specified in the authorization (including provisions of the security plan which may have been made mandatory through the authorization process). In the event that risks are identified, including risks unforeseen in the authorization process, the regulatory body should require operators to take corrective actions.
The response of the regulatory body to non-compliance with regulatory requirements or with any conditions specified in the authorization should be commensurate with the security significance of the non-compliance, in accordance with a graded approach.

Enforcement actions by the regulatory body based on established criteria may include recorded verbal notification, written notification, imposition of additional regulatory requirements and conditions, written warnings, penalties and, ultimately, modification, suspension or revocation of the authorization. Regulatory enforcement may also entail prosecution, especially in cases where the operator does not cooperate satisfactorily in addressing the non-compliance.

At each significant step in the enforcement process, the regulatory body should identify and document the nature of non-compliances and the period of time allowed for correcting them, and should communicate this information in writing to the operator.

The operator should be held accountable for remedying non-compliances, for performing a thorough investigation in accordance with an agreed timetable and for taking all the measures that are necessary to prevent recurrence of the non-compliances.

The regulatory body should confirm that the operator has effectively implemented any necessary corrective actions.

3.3.3. Operator

“The legislative and regulatory framework should require that the operator:

- Comply with all applicable regulations and requirements established by the State and the regulatory body;
- Implement security measures that comply with requirements established by the State and the regulatory body;
- Establish quality management programmes that provide:
  - Assurance that the specified requirements relating to nuclear security are satisfied;
  - Assurance that the components of the nuclear security system are of a quality sufficient for their tasks;
  - Quality control mechanisms and procedures for reviewing and assessing the overall effectiveness of security measure;
- Report to the regulatory body and/or to any other competent authority, all nuclear security events involving radioactive material, associated facilities and associated activities according to national practices;
• Cooperate with and assist any relevant competent authorities in case of a nuclear security event.” (Ref. [3], para. 3.13)

Operators should have the primary responsibility for designing, implementing and maintaining security systems for radioactive material in accordance with regulatory requirements. Operators may be allowed, depending on the applicable regulatory requirements, to contract with a third party to carry out actions and tasks related to the security of radioactive material, although the authorized operator should retain the prime responsibility for regulatory compliance and effectiveness of the actions and tasks. Also, operators should be required to ensure that contractor personnel are suitably trained and meet those regulatory requirements which would apply if such personnel were directly employed by the operator, including requirements pertaining to trustworthiness.

Operators should be required to conduct periodic evaluations to verify that their facilities are in compliance with all applicable security requirements and assess the effectiveness of their security systems to identify any weaknesses that should be corrected and any opportunities for continuous improvement. These evaluations should be based on relevant threat information provided by the regulatory body. These evaluations could take the form of a vulnerability assessment. Details on a vulnerability assessment are provided in Appendix III.

Operators should be required to establish a management system commensurate with the security levels of their radioactive material, to ensure that:

(a) The security system is reliably operated and maintained, functions as intended, is effective, and meets regulatory requirements;

(b) The security system integrates people, procedures and equipment;

(c) Administrative security measures are established to address any identified threats;

(d) Policies and procedures are established that identify security as being of high priority;

(e) Radioactive material is adequately identifiable, traceable, and periodically verified to be present at its authorized location;

(f) Problems affecting security are promptly identified and corrected in a manner commensurate with their importance, including but not limited to:

— Confirmation that security measures, pertaining both to the security system and to security management, are and remain effective as long as radioactive material is present;

— Notification to, cooperation with, and assistance to the regulatory body and other competent authorities in case of security events, as required by legislation or regulation;
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 material is protected in accordance with a security plan.

### 3.4. INTERNATIONAL COOPERATION AND ASSISTANCE

“States are encouraged to cooperate and consult, and to exchange information on nuclear security techniques and practices, either directly or through relevant international organizations.” (Ref. [3], para. 3.14)

Each State should consider whether, and to what extent it may cooperate with other States including the appropriate sharing of information and knowledge derived from its national nuclear security regime, having regard to the sensitive nature of nuclear security information and the need to protect it and share it on the basis of the State’s national legal framework.

States have gained experience with nuclear security and have accumulated both good practices and lessons learned. Sharing these types of information among States can benefit the global community by raising the overall level of security of radioactive material. While some facility specific sensitive information should not be shared, other useful information can be shared in workshops, training programmes, and nuclear security conferences. The IAEA may be a useful vehicle in sharing such information, without attribution.

“States concerned should, in accordance with their national law, provide cooperation and assistance to the maximum feasible extent in the location and recovery of radioactive material to any State that so requests.

“For the purpose of reporting nuclear security events, States should consider establishing suitable arrangements to enable them to participate in relevant regional and international databases and international activities in accordance with their national legislation. One example is the IAEA’s Incident and Trafficking Database (ITDB). Consideration should also be given to other bilateral and multilateral support arrangements.” (Ref. [3], paras 3.15–3.16)

Provision of timely information about missing or stolen radioactive material to neighbouring States and the IAEA is important to assist with its location and recovery. Notification of nuclear security events to neighbouring States and the IAEA may also be useful in identifying and addressing potential threats associated with the radioactive material involved. Information may be provided on a voluntary
basis to the IAEA Incident and Trafficking Database [19]. States may also make use of other
mechanisms the IAEA has established for notifying other States, sharing information, and receiving
financial or technical support in the event of a nuclear or radiological emergency triggered by a
nuclear security event such as the theft of radioactive material [20, 21].

In the case of unauthorized removal of radioactive material, the concerned State would benefit from
assistance from other States to locate and recover the missing radioactive material if it may have
entered or transited through a neighbouring State. Detection of the material will be dependent on a
State’s system for detection of nuclear and other radioactive material out of regulatory control.
Further information on a State’s system for detection of nuclear and other radioactive material outside
of regulatory control is provided in Refs [4] and [22].

State points of contact for nuclear security established in advance of a nuclear security event are
especially important in the case of unauthorized removal or sabotage in order to facilitate prompt and
accurate communication of essential information to neighbouring States and other concerned parties,
either directly or through the IAEA. These contacts may also be useful in communicating other
important nuclear security information, such as new threats.

3.5. IDENTIFICATION AND ASSESSMENT OF THREATS

“The State should assess its national threat for radioactive material, associated facilities and
associated activities. The State should periodically review its national threat, and evaluate the
implications of any changes in the threat for the design or update of its nuclear security regime.”
(Ref. [3], para. 3.17)

3.5.1. National threat assessment

Requirements for the design and evaluation of security systems should take into account the current
national threat assessment and may include the development and application of a design basis threat
(DBT) or alternative threat statement (ATS). Regardless of which method is used, the results define
the capabilities of the adversary, whether an insider or external, that the security system will need to
address.

This process is depicted in Figure 1.
FIG. 1. Process for using threat information.

The national threat assessment is an analysis that documents at a national level the existence, credible motivations, intentions, and capabilities of potential adversaries that could cause harmful radiological consequences through the unauthorized removal of radioactive material or sabotage of radioactive material or an associated facility or associated activity. Depending on the national context, this national threat assessment may be part of a broader threat assessment comprising different sectors. Typically, a national threat 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. The national threat assessment should be updated on a regular basis or when the situation makes it necessary such as the acquisition of new information pertaining to criminal activity.

The national threat assessment may cover the following attributes and characteristics for each identified insider and external adversary, and vary according to national practice:

(a) **Motivation**. Political, financial, ideological, personal.

(b) **Level of commitment**. Disregard for personal health, safety, well-being, or survival.

(c) **Intentions**. Unauthorized removal, material or facility sabotage, public panic and disruption, political instability, mass injuries and casualties, loss of reputation, unavailability of facility, demonstration.
(d) **Group size.** Attack force, coordination, support.

(e) **Weapons.** Types, numbers, availability, improvised.

(f) **Tools.** Mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment.

(g) **Modes of transport.** Land, water, air; type, number, availability.

(h) **Technical skills.** Engineering, use of explosives and chemicals, radiation protection, communication skills.

(i) **Computer skills.** Skills to compromise computer systems and components and the availability, integrity and confidentiality of the data processed, stored or forwarded in computer systems and components.

(j) **Knowledge.** Targets, site plans and procedures, security measures, safety and radiation protection procedures, operations, potential use of radioactive material.

(k) **Funding.** Source, amount, availability.

(l) **Insider issues.** Collusion, passive/active, violent/non-violent, number of insiders.

(m) **Support structure.** Local sympathizers, support organization, logistics;

(n) **Tactics.** Covert and overt.

Once the State has performed a national threat assessment, it will need to decide on the method to be followed for using threat information in establishing regulatory requirements.

One method for using threat information in establishing regulatory requirements is to use the national threat assessment directly. If not previously involved in the national threat assessment, the regulatory body should obtain the results of the national threat assessment for its adoption and use in the development of its regulatory requirements for security of radioactive material, associated facilities and associated activities. Where this method is used, the regulatory body establishes regulations that require the operator to implement security systems which protect against adversary characteristics identified in the national threat assessment.

Another method is to regulate on the basis of a DBT or ATS (see below), for which the national threat assessment becomes an input.

In selecting which method to use, the State should consider several factors, including the severity of consequences associated with malicious acts involving radioactive material in the State, the ability to establish effective protection systems using each regulatory approach, and the ability of the regulatory body to implement the different regulatory approaches.
3.5.2. Design basis threat or alternative threat statement (DBT or ATS)

Development and use of a DBT or ATS differs in two respects from direct use of the national threat assessment for regulatory purposes. First, there is an additional process of screening and decision making. As described more fully in Ref. [23], the process has three major phases:

(a) Screening the threat assessment output for those threats with motivation, intention, and/or capability to commit a malicious act involving radioactive material, associated facilities or associated activities;

(b) Translating the resulting screened list into a statement of representative attributes and characteristics of the postulated adversary;

(c) Modifying the statement of representative threat attributes and characteristics on the basis of relevant policy considerations.

Second, the output of this process is a more detailed and comprehensive set of attributes and characteristics of threats for which the State organizations and the operators have protection responsibilities and accountability.

A DBT and an ATS entail similar steps, but the ATS approach is less rigorous and formal and generally involves fewer organizations. If the State does not have sufficient resources to conduct the formal process of DBT development, or if the DBT process does not bring sufficient benefit in terms of reducing the risk associated with the radioactive materials to be protected, then an ATS can be defined.

It is also possible that a State defines a DBT for high consequence radioactive material, and an ATS for low consequence ones.

The development of a DBT or ATS will be specific to each State, due to social, cultural and geopolitical differences. As with the national threat assessment, developing a DBT or ATS typically requires the combined efforts of domestic authorities such as intelligence and security agencies, law enforcement and the regulatory body and operators, as well as the consideration of policy factors. The State should assign overall responsibility for preparing and maintaining the DBT or ATS to the regulatory body or another competent authority, as appropriate, depending on legislation and other national circumstances. The DBT or ATS should be reviewed from time to time in the light of new information from competent authorities.

Output of DBT or ATS

The primary output of the DBT or ATS process is a document that identifies the set of attributes and characteristics of threats for which the regulatory body, other competent authorities, and operators
have security responsibilities and accountabilities. As discussed in Section 5, the nature of the DBT or
ATS information conveyed to operators will depend on the particular regulatory approach chosen.

**Maintenance of the DBT or ATS**

The responsible regulatory body or other competent authority should establish a formal review
process to maintain the validity of the DBT or ATS. This process should also include provision for
assessment of quickly evolving threats that may need to be addressed on an urgent basis before they
can be incorporated in a revised DBT or ATS. The manner in which such evolving threats are
addressed will vary from State to State.

The responsible regulatory body or other competent authority should determine the frequency of
periodic reviews of the DBT or ATS, depending on such factors as the legislative and regulatory
framework, the stability of the threat environment, the degree of conservatism incorporated in the
ATS and DBT, and available resources. In addition to periodic review, provision should be made for
review of the DBT or ATS based on such events as an event or act that significantly changes the
threat, significant changes in law or policy, or significant new activities involving radioactive
material.

The process and participants in the DBT or ATS review should be the same as for preparation of the
original DBT or ATS, unless changes in law or government organization require alteration of these
arrangements. The output of the review should be a determination as to whether the current DBT or
ATS continues to suffice or a revised DBT or ATS is necessary. If a new DBT or ATS is issued, the
regulatory body should assess its security regulations and their implementation by operators to
determine if amended regulatory requirements or modifications to operators’ security system are
necessary to counter the newly defined threat.

**3.5.3. Insider threats**

The insider threat is often neglected, particularly in radioactive material facilities. Malicious acts can
be caused by internal persons such as disgruntled employees or contractors. Employees may also be
susceptible to coercion and therefore operators should acknowledge this potential vulnerability.
Employees or contractors often are the most aware of vulnerabilities within the facility and have
access to such areas, and therefore it is not enough to simply plan for disruption from outsiders.
Moreover, insiders may take advantage of access rights and knowledge to bypass systems, measures
and procedures for security and safety. Additionally by virtue of access to the facility, the insider has
the ability to use his or her authority to obtain sufficient knowledge about the facility and processes to
identify unique scenarios to successfully complete a malicious act.

There are some tactics, not available to outsiders, that an insider is capable of carrying out in the
course of preparing or conducting a malicious act. These include, for instance, compromising security
by manipulating people or adjusting a security system to perform in a manner different from the way
it was intended in order to learn useful information. Moreover, individuals may seek employment at a
facility with the intention of committing malicious acts and may also assist external adversaries to
remove radioactive material or carry out hostile acts.

The national threat assessment, DBT, and/or ATS as applicable, should address the insider threat.

The general methods described in Ref. [24] may be applied, using a graded approach, to measures
against insider threats in relation to radioactive material and associated facilities. Insider threats are
addressed through technical measures such as video surveillance and accounting, as well as security
management measures, such as access control, trustworthiness verification, and information
protection. A robust nuclear security culture, which includes nuclear security awareness and reporting
of nuclear security events, is an important means of countering insider threats.

3.5.4. Increased threat

A security system should be effective in countering the threat derived from the national threat
assessment, or as determined by the DBT or ATS, as applicable. However, the regulatory body should
also establish arrangements to ensure that security systems can be temporarily strengthened during
times when the threat suddenly increases. These arrangements should include requirements for
operators to introduce additional security management measures to counter increased threats. Such
measures should be periodically tested and included in the operator’s security plan.

3.5.5. Protection against threats beyond the DBT or ATS

A secondary result of the DBT or ATS process is identification of those threats for which protection
should be provided but which it is not reasonable to require operators to protect against, generally
because the capabilities necessary to counter such threats are beyond the capacity of operators. Such
threats are generally countered by the State, and are not included in regulatory requirements.

3.5.6. Evaluation methods

There are a number of evaluation methods for assessing the effectiveness of a security system in
protecting against the threat. One such method is by means of a vulnerability assessment (VA). The
VA can be specific or general in nature, and can be conducted by the operator to demonstrate system
effectiveness (compliance) against the requirements specified in the State’s regulatory framework or
by the State’s regulatory body to verify the operator’s compliance. Vulnerability is assessed against
the basic security functions (detection, delay and response) to ensure that the risks associated with
malicious acts against radioactive material and associated facilities, as defined by the State, are
managed to an acceptable level. The basic security functions are further explained in Section 4 of this implementing guide. Additional information on how to conduct a VA can be found in Appendix III.

3.6. RISK BASED NUCLEAR SECURITY SYSTEMS AND MEASURES

3.6.1. Risk management

“The State should follow a structured risk management approach to reduce the risks of malicious acts to an acceptable level. The State should assess the potential threats, the potential consequences and the likelihood of malicious acts, and then develop a legislative and regulatory framework that provides for efficient and effective security measures to address the threat.

“The State should decide what level of risk is acceptable and what level of effort is justified to protect radioactive material, associated facilities and associated activities against the threat so as to reduce the risk to an acceptable level, given the availability of resources, the benefit of the protected asset to society, and other priorities. The required security measures may take advantage of other measures established for radiological safety purposes.” (Ref. [3], paras 3.19–3.20)

Security risk is the qualitative or quantitative expression of possible harm that considers the threat, the likelihood that malicious acts could be successfully carried out by this threat against a specific target, and the potential harmful radiological consequences of those acts.

In addition to harmful radiological consequences, a malicious act could have multiple indirect consequences such as a mass panic, psychological effects, loss of confidence in the radioactive material industry, etc. While recognizing that all of these consequences may exist, this publication only takes into account the harmful radiological consequences of a malicious act in the risk management process. However, States may consider these other indirect consequences when defining the acceptable level of risk within their territory.

The State should use a risk management approach to ensure that its security requirements keep the risk of unauthorized removal or sabotage at an acceptable level.

This approach consists of evaluating the threat and potential harmful radiological consequences of malicious acts and ensuring that appropriate security measures are put into place to reduce the likelihood of a successful malicious act sufficiently to bring the risk to an acceptable level.

To achieve this result, the likelihood of adversary success needs to be reduced as the degree of harm rises. In other words, the greater the harmful radiological consequences resulting from a malicious act involving particular radioactive material, the more effective the security system needs to be. This principle is reflected in Section 5 below, which recommends that the regulatory body establish three graded security levels for radioactive material, each with a required degree of security system effectiveness, and that the regulatory body assign radioactive material to a given security level.
primarily based on the potential harmful radiological consequences resulting from successful use of
that material in a malicious act.

“The regulatory body should establish regulations based on a prescriptive approach, a performance
based approach or a combined approach in order to achieve the objectives of the nuclear security
regime, as discussed in paras 4.6 and 4.7.” (Ref. [3], para. 3.21)

There are three approaches that the regulatory body may use as a basis for security regulations. The
approach 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 material that should
be secured.

A prescriptive approach establishes a set of specific security measures determined by the regulatory
body to provide an acceptable level of security against the defined threat. The prescriptive approach
has the advantage of simplicity in implementation, both for the regulatory body and for operators. The
disadvantage of this approach is its relative lack of flexibility to take into account specific
circumstances. For example, an operator’s security system could be in compliance with prescriptive
requirements, but not fully address the actual vulnerabilities of the operator’s radioactive material
against particular threats.

A performance-based approach is one in which the regulatory body allows flexibility for the operator
to propose the particular combination of security measures that will be used to achieve a required
level of performance. 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 greater flexibility of the performance-based approach also reduces
the need for changes to regulations when new requirements are identified by the regulatory body. The
prerequisite for this approach is that it requires both the operator and the regulatory body to have
relatively high levels of security expertise.

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
material with the greatest potential for harmful radiological consequences from malicious use and a
prescriptive approach for material with less potential for harmful radiological consequences. The main
advantage of the combined approach is the flexibility it allows the regulatory body in adjusting
regulatory requirements to meet specific needs and constraints.

The three approaches are discussed in further detail in Section 6.
“The State should consider ways of reducing the nuclear security risk associated with radioactive material, particularly radioactive sources, for example by encouraging the use of an alternative radionuclide, chemical form, or non-radioactive technology, or by encouraging device designs that are more tamper resistant.” (Ref. [3], para. 3.22)

Consideration should be given to encouraging the use of newly developed or existing alternative technologies or operational practices in any application where the alternative technology or practice may reduce the security risk associated with this radioactive material.

These technologies or practices, where technically and economically feasible, could rely, for example, on the use of:

(a) Another form of the same radionuclide. For example, the use of caesium ceramics rather than caesium chlorides;

(b) An alternative radionuclide. For example, 3H has been used in radioluminescent devices in place of the traditionally used 226Ra.

(c) A non-radioactive technology. For example, 60Co teletherapy devices may be replaced by linear accelerators in some cases.

(d) Non-radiological techniques. For example, the use of electronic gauges instead of level or density gauges containing 137Cs or 60Co sources.

(e) Modified operational practices. For example, in industrial radiography, moving the item to be tested from the job site to a secure permanent facility.

In addition to alternative technologies, consideration should be given to the use of more tamper-resistant designs for devices using radioactive material which can be used to increase the time it takes to access and remove radioactive material from a device. The addition of hardware such as difficult-to-penetrate plates to armour up vulnerable maintenance locations can be considered. The use of speciality fasteners that require specialized tools to install and remove can be a valuable measure as well. The additional delay time provided by these measures can give response forces needed time to respond to an attempted unauthorized removal of radioactive material.

When investigating potential substitutes for radioactive material, all advantages and drawbacks should be taken into account. For example, X-ray devices usually rely on a dedicated power supply and a cooling system that might not be always available. The reliability of alternative technologies may not be sufficient in every situation.

States should exchange information in this regard. For example, when the security of a device design has been enhanced in one State, other States could benefit from this enhancement on their territory.
“The regulatory body should develop requirements by using a graded approach applying the principles of risk management including a categorization of radioactive material.” (Ref. [3], para. 3.23)

Security-based Categorization refers to the process of categorizing radioactive material based on its activity level and/or use, assigning an appropriate security level, and making adjustments to the security level and resulting security measures based on specific factors or considerations. The process is illustrated in Figure 2.

For protection against unauthorized removal of radioactive material or against sabotage, the State should consider the potential harmful radiological consequences of such acts and apply a graded approach when developing regulatory requirements.

“The regulatory body should develop requirements based on the concept of defence in depth. Security requirements for radioactive material require a designed mixture of hardware (security devices), procedures (access control, follow-up, etc.) and facility design.” (Ref. [3], para. 3.24)

The regulatory body should require that the defence-in-depth approach is incorporated in the design of the security system for the functions of detection, delay and response. Within each function, to the extent appropriate given the graded approach, the system design should have independent capabilities so that failure of one capability does not mean loss of that function. For example, detection can rely on observation by personnel and also use electronic measures to detect intrusion into the facility. Delay can consist of multiple, independent and diverse physical barriers that must be overcome to gain access to the target, such as fences, barricades, hardened buildings, hardened doors, cages and tie-downs so the adversary task time is increased. Response can consist of on-site guards and local police response.

Combining the principles of graded approach and defence in depth, for higher consequence targets, the security measures for detection, delay, and response may use more layers and may use more effective components.
3.6.2. Interfaces with the safety system

“Recognizing that both safety and security have a common aim — to protect persons, society and the environment from harmful effects of radiation — a well-coordinated approach in safety and in security is mutually beneficial, the State should ensure that:

- Consultation and coordination are maintained between those responsible for safety and security to ensure efficient security of radioactive material and to ensure that regulatory requirements are consistent, especially when responsibility for safety and security is assigned to different competent authorities;
- Major decisions regarding safety and security require participation of experts in safety and in security on a continual basis;
- The safety and security interfaces should be strengthened by building safety culture and nuclear security culture into the management system.

“The State should ensure that a balance is maintained between safety and security throughout the nuclear security regime, from the development of the legislative framework to implementation of security measures.

“The competent authorities should ensure that security measures for radioactive material, associated facilities and associated activities take into account those measures established for safety and are developed so that they do not contradict each other, during both normal and emergency situations.

“The competent authorities working with the operator should ensure to the extent possible that security measures during a response to a nuclear security event do not adversely affect the safety of the personnel. Security personnel should manage their actions in a way that maintains the safety of all potentially affected persons, whether on or off-site.” (Ref. [3], paras 3.25–3.28)

The interfaces between safety and security should be taken into account at both State and operator levels.

State

The nuclear safety system and the nuclear security system for radioactive material and associated facilities both include authorization, inspection and enforcement processes. Consequently, the legislative and regulatory framework for the security of radioactive material should take into account the pre-existence of the legislative and regulatory framework for safety, including emergency preparedness and response, and radiation protection.

Assigning the responsibility for both safety and security to a single regulatory body could help optimize resources and facilitate an integrated system of protection and control through authorization,
inspection and enforcement processes. It would also make it easier for the regulatory body to take account of both safety and security issues when developing regulations.

There should be regular, systematic cooperation and information sharing between the organizational units responsible for the development and implementation of safety and security requirements. This information sharing and the decision making process could include, but is not limited to:

(a) Consideration of safety and security in the respective authorization processes, including during categorization of radioactive material and inclusion of requirements for accounting and inventory;

(b) Common inspections, as much as the protection of information allows for it;

(c) Assessment of the emergency plans and security plans provided by the operators within their application;

(d) Involvement of safety specialists in the development of security requirements, and vice versa; and

(e) Working groups dealing with specific technical interfaces.

In addition to the regulatory bodies, these working groups could include, as appropriate, the intelligence community, ministries of interior, defence, transportation, and foreign affairs; law enforcement; customs and coast guard and other agencies with security related responsibilities and the ministries of health, environment or other agencies with safety, health, or emergency preparedness and response-related responsibilities; senior management meetings to deal with major issues such as import/export controls; and as appropriate, ministerial arbitration in case of a remaining disagreement.

In all cases, there is a need to develop dedicated methods to ensure the transparency of information pertaining to safety issues and to protect the information that is of a security concern. The interface between safety and security will require the building of an integrated safety and security culture within the regulatory body. Technical solutions will need to be developed in order that personnel with responsibilities for safety and security all have appropriate access to information needed fulfil their duties such as the data of the national inventory of radioactive material.

The interface between safety and security at the State level is depicted in Figure 3.
Operators

The operator has the primary responsibility for the safety and security of radioactive material. A good practice for establishing and maintaining an effective interface between safety and security is to implement safety and security in such a way that they are mutually supportive. For example, safety procedures to prevent safety incidents may also support security.

In many cases, the operator’s staff dealing with safety issues will also deal with security aspects. In those cases, the integration of safety and security will be more easily achieved.

For those cases when safety and security are not dealt with by the same staff within the operator’s organization, safety and security specialists should be organized in such a way as to manage the interfaces between safety and security. Senior management should participate in safety-security interface meetings and ensure that neither safety nor security is compromised by the other. Outputs of safety-security interface meetings should be recorded. Security staff should have adequate knowledge of radiation protection requirements and similarly, safety staff should be familiar with those security measures that are implemented in their work environment.

Specific examples where safety–security interfaces should be addressed include:

(a) Maintenance of a device containing radioactive material;
(b) Replacement of radioactive material;
(c) Performing radioactive material inventories;
(d) Any change in the safety or security system or in the design/characteristics of the facility (location of radioactive material, type of devices, access control, etc.). Such changes should always be analysed from both points of view before being implemented. Where
potential adverse impacts are identified, the operator should communicate them to appropriate personnel within the organization and consider alternative measures or take compensatory and/or mitigating actions.

(e) Access control and access to information.

(f) Consideration of the radiation protection programme in the development of the security plan.

The operator should recognize safety-security interface issues and manage them appropriately during normal operations as well as during emergencies. Emergencies, whether due to a safety event or a security event, are of a particular concern and the interfaces should include, for example:

(a) Ensuring, as far as possible, that necessary emergency arrangements have been taken into account in the development of the security system;

(b) Coordinating and integrating security plans with emergency plans;

(c) Developing and conducting regular exercises to test the coordinated plans and arrangements;

(d) Ensuring, as far as possible, that security response forces have adequate knowledge of radiation protection, and that they are designated, depending on their duties, as emergency workers and appropriately protected as required by Refs [10], [11] and [25];

(e) Maintaining security to the extent possible during an emergency;

The interface between safety and security at the operator level is depicted in Figure 4.

3.7. SUSTAINING THE NUCLEAR SECURITY REGIME

“The State should commit the necessary resources, including human and financial resources, to ensure that its nuclear security regime is sustained and effective in the long term to provide adequate nuclear security for radioactive material.

“The State should promote a nuclear security culture.

“All organizations and individuals involved in implementing nuclear security should give due priority to the nuclear security culture with regard to radioactive material, to its development and maintenance necessary to ensure its effective implementation in the entire organization.

“The foundation of a nuclear security culture should be the recognition that a credible threat exists, that preserving nuclear security is important, and that the role of the individual is important.” (Ref. [3], paras 3.29–3.32)

If the nuclear security regime is to remain effective it needs to be sustained over time at both the national and operational levels. Ref. [9] indicates that sustainability is “the set of principles and implementing actions incorporated into the nuclear security regime that support its continuing effectiveness against a defined threat,” at both the national and operational levels. The following paragraphs summarize some of the key principles and actions in that publication that are particularly relevant to the security of radioactive material. More detailed guidance is provided in Ref. [9].

3.7.1. National level

The national level refers to those elements of the nuclear security regime addressed by the State and its competent authorities that have general, State-wide applicability.

The State should build and maintain a national commitment to nuclear security. As national leadership changes over time, the commitment to the nuclear security regime should be reaffirmed as a national priority and maintained through the legislative, regulatory and administrative framework.

The State and its competent authorities should regularly review, and if necessary update, the legislative and regulatory framework for the nuclear security regime, to ensure that it remains appropriate, effective, consistent and coherent.

The State should define roles and responsibilities and ensure accountability of competent authorities in meeting those responsibilities. Reallocation of responsibilities may be necessary to address new issues or State-level reorganization of the nuclear security regime. In the interest of promoting stability and certainty, reallocation of responsibilities should only be undertaken when essential.

The State and its competent authorities should periodically update the national threat assessment to ensure the continuing relevance of nuclear security requirements for radioactive material.
The State and competent authorities should conduct effective planning and organization to ensure the continued availability of appropriate human, financial, and technical resources over the long term. The State and its competent authorities should create and cultivate indigenous training institutions, such as dedicated training departments within competent authorities, and other training centres. Such mechanisms help ensure that training in nuclear security is enduring, rigorous, relevant to national conditions, and responsive to evolving needs.

The State should maintain oversight of and regularly evaluate the nuclear security regime in order to measure and gauge its effectiveness to ensure that it continues to meet national objectives. This function could be performed, for example, through the establishment of a national oversight and review committee.

### 3.7.2. Operational level

The operational level includes those nuclear security systems implemented at a facility or in connection with any other activity where radioactive material is present. The following are key actions that operators should take in order to sustain their security systems. Most of these actions should be required by the regulatory body in regulations or conditions of authorization.

Operators should set priorities, identify long-term financial resources, and define roles, responsibilities and accountabilities for nuclear security and document these decisions in appropriate plans, including a security plan.

Operators should establish and document a systematic process for maintaining and acting on current threat information.

Operators should assign and document all nuclear security responsibilities, establish the number of staff required, and define the qualifications and competencies for each position. To ensure that staff with security responsibilities remain appropriately trained and qualified, operators should provide for the continuous development and renewal of trained and qualified staff.

Operators should establish, implement, document and periodically review and update as appropriate a maintenance programme for security systems and equipment. Operators should apply configuration management to document the physical, procedural and training elements of its critical nuclear security systems.

Operators should implement formalized and documented compliance and performance evaluations, including periodic performance tests and exercises, both internally and with external response organizations. Operators should document results of evaluations, including corrective actions, and where appropriate report the results and findings to the regulatory body.
Operators should promote a dynamic and effective security culture all levels of operator staff and management by such means as:

(a) Assigning responsibility for the security of radioactive material to a senior staff member, but ensuring that staff members are aware that security is a shared responsibility across the whole organization;

(b) 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;

(c) Ensuring threat awareness and training of security managers, response personnel and all personnel with secondary responsibilities for security;

(d) Addressing security matters in staff and contractor orientation courses;

(e) Providing security instructions and ongoing security awareness briefings to staff and contractors, and training and evaluation of the lessons learned;

(f) Conducting security culture surveys and using the results to address identified problems.

Ref. [26] describes the basic concepts and elements of security culture.

3.8. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

“The regulatory body should ensure that the operator’s security plan includes measures to effectively respond to a malicious act consistent with the threat.” (Ref. [3], para. 3.33)

The regulatory body should require the operator to include in its security plan measures which ensure a timely and effective response to a suspected, attempted or actual malicious act involving radioactive material within the facility.

Operators have responsibilities for facility-specific response measures; however any event with off-site consequences should be managed in a coordinated and integrated way taking into account all organizations involved. The regulatory body should further ensure that response measures in the operator’s security plan are consistent with those developed at the State and local level.

Arrangements should be made to ensure, as far as practicable, the continued effectiveness of the security system during any response, including careful coordinated and integrated planning by the State, regulatory body, operator, and other local/national response authorities, in the development and exercise of appropriate response measures.

Response measures should be developed taking into consideration foreseeable scenarios based on threat information. These measures should be periodically exercised, reviewed and revised as
necessary. They should be made enforceable, for example by inclusion in the authorization conditions.

Operators’ security plans should take into account emergency arrangements established to effectively respond to a nuclear or radiological emergency in line with Refs [10], [11] and [25], and based on a graded approach.

3.9. IMPORT AND EXPORT OF RADIOACTIVE MATERIAL

“The State should take appropriate steps, including coordination between importer and exporter States prior to the transfer, to reduce the likelihood of malicious acts in connection with the import or export of quantities of radioactive material above thresholds that it defines. At a minimum, these steps should encompass requirements concerning Category 1 and 2 sealed radioactive sources, consistent with the Guidance on the Import and Export of Radioactive Sources.” (Ref. [3], para. 3.34)

Import–export control serves several important security-related purposes:

(a) To increase importing State awareness of the import of high activity sources, with corresponding safety and security risks;

(b) To ensure that sources do not fall out of regulatory control during the export-import process and thus risk becoming lost, abandoned, or stolen; and

(c) To ensure that exported sources are safely and securely managed throughout their lifecycle.

Consistent with the Code of Conduct and the Guidance on the Import and Export of Radioactive Sources, the State should authorize and require the regulatory body or other competent authority to establish and implement a system for controlling the import and export of at least all Category 1 and 2 radioactive sources. States may consider extension of such measures to exports or imports of other radioactive material on a risk-informed basis.

This system should include, as applicable:

(a) Nominating a point of contact for facilitating import-export control of radioactive material;

(b) Establishing procedures for the authorization and control of imports and exports, which allow such imports and exports only if:

- The recipient is authorized by the importing State to receive and possess the radioactive material;

- The importing State has the capability for safe and secure management of the radioactive material;
• The exporting State has sought and received the importing State’s consent to the import Category 1 radioactive sources only;

• The exporting State has notified the importing State prior to shipment.

(c) Providing for consideration of authorizing imports and exports if one or more of the foregoing provisions cannot be followed due to exceptional circumstances;

(d) Submitting the State’s responses to the Importing and Exporting State Questionnaire, as well as any updates of those responses to the IAEA through official channels.

3.10. DETECTION OF NUCLEAR SECURITY EVENTS

“The regulatory body should establish requirements for operators to have appropriate and effective security measures to detect nuclear security events and to report any such event promptly with the aim of providing a timely response. These requirements should consider those made in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control.” (Ref. [3], para. 3.35)

Detection is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal of radioactive material or sabotage, as well as the discovery of actual loss or removal of radioactive material or an act of sabotage. Detection can occur either within the facility or outside of the facility.

The regulatory body should require the operator to establish, test and implement detection and response measures, on a graded basis and in cooperation with State and local level emergency and response plans. These measures should be documented in the operator’s security plan or in a standalone response plan.

Where nuclear security activities involving radioactive material out of regulatory control are concerned, the regulatory body should have in place regulations that require the operator to coordinate with the relevant competent authorities where response actions are required.

The regulations should also include requirements for the operator to report nuclear security events that are detected, addressing such matters as:

(a) Procedures for determining whether the event detected is a nuclear security event;

(b) Timely reporting to the regulatory body, the competent authority with responsibilities for radiological emergency response, and law enforcement, as appropriate;

(c) Taking appropriate action to remedy or mitigate the circumstances; and

(d) Investigating the event and its causes, circumstances, actual and potential consequences, to prevent a recurrence of similar situations;
(e) Within a specific time period, providing the regulatory body with a report on the causes of the event, its circumstances and consequences, and on the corrective or preventive actions taken or to be taken.

4. SECURITY CONCEPTS

This section introduces and explains key security concepts, including the basic security functions of deterrence, detection, delay, response, and security management.

4.1. PURPOSE OF A SECURITY SYSTEM

A security system is an integrated set of nuclear security measures intended to prevent the completion of a malicious act. Such an act would consist of a sequence of actions by adversaries to obtain access to radioactive material for the purpose of either sabotage or unauthorized removal.

The security system should be designed by the operator to deter adversaries from attempting a malicious act and to prevent adversaries from completing such a malicious act through detection, delay, and response measures. The security system should also include security management measures for the integration of people, procedures, and equipment through the application of administrative measures.

4.2. SECURITY FUNCTIONS

Deterrence

Deterrence occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt. Deterrence measures have the effect of convincing the adversary that the completion of the malicious act would be too difficult, the success of the act too uncertain, or the penalties too severe to justify the undertaking. Deterrence measures thus include making the adversary aware of the presence of measures performing the other security functions. If this communication has the intended effect, deterrence is the result. However, there should be some caution in communicating details of security measures which could enable adversaries to circumvent or defeat the security system. Regulatory bodies and operators should consider how to balance this risk with the deterrent value of alerting the adversary to the presence of security measures to the adversary.

Detection

Detection is a process that begins with sensing a potential malicious act and that is completed with an assessment of the cause of the alarm.
Detection and assessment can be achieved by several means. Sensing unauthorized access can be accomplished through such means as electronic sensors or visual observation. Sensing unauthorized removal can be accomplished through such means as tamper-detection devices or visual observation or, after the fact, by accountancy records. Assessment can be performed through such means as remote video monitoring or visual observation.

**Delay**

Delay impedes an adversary’s attempt to gain unauthorized access to a location where radioactive material is present, or to remove or sabotage radioactive material, generally through barriers or other physical means. A measure of delay is the length of time, after detection, that is required by an adversary to remove or sabotage the radioactive material.

**Response**

Response encompasses the actions undertaken following detection to prevent an adversary from succeeding in unauthorized removal or sabotage. These actions, which may be performed by on-site guards or by off-site law enforcement, security or military personnel, have the objective of interrupting and defeating an adversary while the attempted unauthorized removal or sabotage is in progress in order to prevent its completion. Effective response requires advance coordination between the operator and off-site responders.

**Security management**

Security management addresses the establishment and implementation of policies, plans, and procedures, and the deployment of the necessary resources, for the security of radioactive material and associated facilities. Security management includes measures for access control, trustworthiness verification, information protection, preparation of a security plan, training and qualification of personnel, accounting, inventory and event reporting.

4.3. DESIGN AND EVALUATION OF SECURITY SYSTEMS

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

*Detection before delay:* The function of delay is to provide response personnel with sufficient time to deploy and interrupt the adversary’s efforts to complete a malicious act. Therefore, detection needs to precede delay. If an adversary is given the opportunity to overcome barriers and other obstacles prior to encountering intrusion sensors or other means of detection, the adversary will have completed some of the necessary tasks before being detected and thus may succeed in removing or sabotaging the radioactive material before response personnel arrive. In this case, barriers do not provide delay but rather, at most, deterrence.
Detection requires assessment: Most means of detection provide an indirect indication of a potential malicious act. 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 or through use of remote video systems. To prevent adversaries from exploiting any delay between detection and assessment, immediate assessment should be the goal of any security system.

Delay time should be greater than assessment time plus response time: A security system is successful if detection and assessment occur quickly enough for subsequent delay measures to permit response personnel to interrupt the adversary prior to completion of the unauthorized removal or sabotage. This relationship of the functions of detection, delay and response is known as timely detection.

Response should be adequate as well as timely: In addition to arriving in time to interrupt the adversaries, response personnel need to have sufficient capability to defeat the adversaries. In other words, there should be a sufficient number of response personnel with the tactics, skills and training necessary to defeat adversaries possessing the capabilities identified in relevant threat information.

Balanced protection: A security system should be designed to provide adequate protection against all defined threats along all possible adversary pathways to the target. In other words, along any possible pathway, detection measures, delay times, and resulting responses should combine to protect the target.

Defence in depth: A security system should employ several layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by adversaries in order to achieve their objective.

5. ESTABLISHING A REGULATORY PROGRAMME FOR THE SECURITY OF RADIOACTIVE MATERIAL

Many States already have a regulatory programme in place that covers activities such as authorization, inspection and enforcement. This section provides guidance to regulatory bodies on how to develop or enhance regulatory programmes to address the security of radioactive material in order to reduce the likelihood of malicious acts sufficiently to bring security risk to an acceptable level. 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 material involves three basic steps for the regulatory body:
(a) **Step 1:** Establish graded security levels, with corresponding goals and objectives for each security level (see Section 5.1).

(b) **Step 2:** Determine the security level applicable to given radioactive material (see Section 5.2).

(c) **Step 3:** Establish regulatory requirements, using a prescriptive, performance-based, or combined approach (see Section 5.3).

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

As explained in Section 3, application of the risk management approach entails basing the required degree of security system effectiveness primarily on the harmful radiological consequences that would result from a successful malicious act involving the particular radioactive material to be protected. Three security levels (A, B, and C) have been developed to allow specification of security system performance in such a graded manner. Security level A requires the highest degree of security system effectiveness while Security levels B and C require progressively less stringent degrees of protection.

The required security system performance is expressed as a goal. The goal defines the overall result that the security system should be capable of providing for radioactive material in that security level. The following goals have been developed:

(a) **Security level A:** Very high level of confidence that the security system will prevent unauthorized removal of radioactive material.

(b) **Security level B:** High level of confidence that the security system will prevent unauthorized removal of radioactive material.

(c) **Security level C:** Confidence that the security system will prevent unauthorized removal of radioactive material.

Malicious acts can involve either unauthorized removal of radioactive material or sabotage. It is important to note that the security goals and recommended measures described in this guidance only focus on unauthorized removal of radioactive material; however, a security system whose performance achieves the applicable goal will also provide some capability to counter sabotage. If the regulatory body becomes aware of a specific threat of sabotage against particular radioactive material or particular facilities, the regulatory body should require additional or more stringent security measures to increase the level of protection against sabotage.

In order to meet the applicable goal, the security system needs to achieve an adequate level of performance for each of the security functions: 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 required outcome from the combination of measures applied for that objective. Deterrence achieved by a security system is difficult to measure. Consequently, it has not been assigned a set of objectives and measures in this publication.

Security levels and associated goals and objectives are summarized in Table 3.

Where an objective is shown in Table 3 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 3. SECURITY LEVELS AND SECURITY OBJECTIVES

<table>
<thead>
<tr>
<th>Security Functions</th>
<th>Security Level A (Goal: Very high level of confidence that the security system will prevent unauthorized removal of radioactive material)</th>
<th>Security Level B (Goal: High level of confidence that the security system will prevent unauthorized removal of radioactive material)</th>
<th>Security Level C (Goal: Confidence that the security system will prevent unauthorized removal of radioactive material)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Provide immediate detection of any unauthorized access to locations where radioactive material is present</td>
<td>Provide immediate detection of any attempted unauthorized removal of radioactive material, including by an insider</td>
<td>Provide detection of any attempted unauthorized removal of radioactive material</td>
</tr>
<tr>
<td></td>
<td>Provide immediate assessment of detection</td>
<td></td>
<td>Provide detection of unauthorized removal of radioactive material</td>
</tr>
<tr>
<td>Delay</td>
<td>Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal of material</td>
<td>Provide delay with high level of confidence that the security system will prevent the unauthorized removal of material</td>
<td>Provide delay with confidence that the security system will prevent the unauthorized removal of material</td>
</tr>
<tr>
<td>Response</td>
<td>Provide immediate communication to response personnel</td>
<td>Provide immediate initiation of response to interrupt unauthorized removal of radioactive material</td>
<td>Implement appropriate action in the event of unauthorized removal of radioactive material</td>
</tr>
<tr>
<td></td>
<td>Provide for immediate response with sufficient capability to interrupt and defeat the adversary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td>Establish a process for granting individuals authorized unescorted access to radioactive material and/or access to sensitive information</td>
<td>Ensure trustworthiness and reliability of authorized individuals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure training and qualification of individuals with security responsibilities</td>
<td>Provide access controls that effectively restrict access to radioactive material to authorized persons only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct accounting and inventory of radioactive material</td>
<td>Identify and protect sensitive information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct evaluation for compliance and effectiveness, including performance testing</td>
<td>Provide a security plan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Establish a capability to manage and report security events</td>
<td>Ensure training and qualification of individuals with security responsibilities</td>
<td></td>
</tr>
</tbody>
</table>

*Achievement of these goals will also reduce the likelihood of a successful act of sabotage.*
5.2. STEP 2: DETERMINE THE SECURITY LEVEL APPLICABLE TO RADIOACTIVE MATERIAL: SECURITY-BASED CATEGORIZATION

In order to specify an appropriate security level for radioactive material, consideration should be given to the potential harmful radiological consequences that this material could cause if it were used in a malicious act. This potential for harmful radiological consequences should then guide the process of assigning an appropriate security level to the radioactive material, and making adjustments to the security level based on specific factors or considerations. This process should consist of the following steps:

(a) Categorizing radioactive material based on the potential to cause harmful radiological consequences if used in a malicious act (including aggregation of radioactive material in a given location as appropriate) (see Section 5.2.1);

(b) Assigning an appropriate security level to each category (see Section 5.2.2);

(c) Adjusting the security level based on specific factors or considerations (see Section 5.2.3)

This guidance recommends an approach to be applied to all radioactive material, including radioactive sources, unsealed radioactive material, and radioactive waste, recognizing that it is designed for radioactive sources, and should therefore be adapted where possible to suit the particular circumstances.

5.2.1. Categorization

The purpose of categorizing radioactive material is to provide a basis for risk informed decision making, including requirements for security measures to reduce the likelihood of successful malicious acts. The IAEA’s recommended categorization system described below is concerned with radioactive sources. This method may also be adapted for application to other radioactive material depending on national considerations.

In order to assign appropriate security levels to radioactive material, it is first necessary to categorize the material based on its potential to cause harmful radiological consequences if used in a malicious act. The recommended IAEA categorization system is based on a set of D-values corresponding to “the quantity of radioactive material, which, if uncontrolled, could result in the death of an exposed individual or a permanent injury that decreases that person’s quality of life” [11, 27]. The D-values for radioactive material were developed for the purpose of establishing requirements for an adequate level of preparedness for and response to a nuclear or radiological emergency, but take into account a number of defined exposure scenarios. These include those security scenarios resulting from the malicious use of radioactive material described in Section 2 such as use in an RDD, placement of an
unshielded source in a public area (an RED), and placement of radioactive material in a food or water supply.

For those scenarios in which the radioactive material is not dispersed, a D1 value for radionuclides was calculated, which is the “activity of a radionuclide [in a source] that if uncontrolled, but not dispersed ... might result in an emergency that could reasonably be expected to cause severe deterministic health effects”.

For those scenarios in which the radioactive material is dispersed, a D2 value, “the activity of a radionuclide [in a source] that if uncontrolled and dispersed might result in an emergency that could reasonably be expected to cause severe deterministic health effects”, was calculated.

Since there was a need for a categorization system for radioactive sources based upon the potential for sources to cause deterministic health effects, the D-values were also used as normalizing factors in generating a numerical relative ranking of sources and practices. Thus, the D-values are also used as the basis for the IAEA Safety Guide [28]. The D-values used in Ref. [28] are the more stringent of the D1 and D2 values calculated in Ref. [27].

The categorization system has five categories. 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 source may be fatal. At the lower end of the categorization system, sources in Category 5 are the least dangerous; however, even these sources should be kept under appropriate regulatory control.

Radioactive material is categorized by taking the activity A of the radioactive material (in TBq) and dividing it by the D value for the relevant radionuclide. The A/D value is referred to as the activity ratio. The category of radioactive material, ranging between 1 and 5, is then assigned based on the value of the activity ratio.

For example, a blood irradiator containing a Cs-137 source has an activity level of 260 TBq. The D-value of Cs-137 is 0.1 TBq. Therefore, taking the A/D ratio, $260 \text{ TBq} / 0.1 \text{ TBq} = 2600$. This means the A/D ratio $\geq 1000$, so the radioactive source would be assigned to Category 1.

A State may choose to employ a different approach (e.g. consider different exposure pathways, dose rates) than the one used to calculate the D-values described in Ref. [27] in order to categorize radioactive material for the purpose of assigning a security level.

While it may be appropriate to categorize radioactive material on the basis of A/D ratio, it may also be convenient to assign a category on the basis of the intended application of the radioactive material [28]. Table 4 provides examples of categorization of radioactive material based on its application. For example, a blood irradiator might be assigned to Category 2 based on the A/D ratio, but assigned to Category 1 based on practice.
### TABLE 4. CATEGORIES OF RADIOACTIVE MATERIAL FOR COMMON APPLICATIONS

<table>
<thead>
<tr>
<th>Category</th>
<th>Activity Ratio (A/D)</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A/D ( \geq 1000 )</td>
<td>Radioisotope thermoelectric generators (RTGs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Irradiators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Teletherapy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fixed multibeam teletherapy (gamma knife)</td>
</tr>
<tr>
<td>2</td>
<td>1000 &gt; A/D ( \geq 10 )</td>
<td>Industrial gamma radiography</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High/medium dose rate brachytherapy</td>
</tr>
<tr>
<td>3</td>
<td>10 &gt; A/D ( \geq 1 )</td>
<td>Fixed industrial gauges that incorporate high activity sources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Well logging gauges</td>
</tr>
<tr>
<td>4</td>
<td>1 &gt; A/D ( \geq 0.01 )</td>
<td>Low dose rate brachytherapy (except eye plaques and permanent implants)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Industrial gauges that do not incorporate high activity sources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bone densitometers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Static eliminators</td>
</tr>
<tr>
<td>5</td>
<td>0.01 &gt; A/D and A &gt; exempt</td>
<td>Low dose rate brachytherapy eye plaques and permanent implant sources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X ray fluorescence (XRF) devices containing a radioactive source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electron capture devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mossbauer spectrometry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Positron emission tomography (PET) check sources</td>
</tr>
</tbody>
</table>

The Code of Conduct on the Safety and Security of Radioactive Sources [5] applies to radioactive sources that may pose a significant risk to individuals, society, and the environment, i.e. Category 1-3 radioactive sources. These radioactive sources, their D-values, and activity thresholds for Categories 1–3 are listed in Table 5, which appears in Annex I of the Code. This set of radionuclides was devised based on national experiences and widespread uses of radioactive material at the time of the Code’s publication in 2004 and it is recommended that, as a minimum, this guidance should be applied to those radionuclides. The list of radionuclides provided in Table 5 should not be viewed as static, and may be modified to reflect fluctuations in industry and new needs which may evolve. For radionuclides not found in this table, the recommended D-values may be found in Ref. [27]. The regulatory body may assign a category to these radionuclides based on the A/D ratio.

---

1. This column can be used to determine the category of radioactive material 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 radioactive material has a short half-life and/or are unsealed, or if radioactive material is aggregated (see Ref. [3], paragraph 3.5).
2. Factors other than A/D alone have been taken into consideration in assigning these applications to a category (see Ref. [3], Annex I).
3. Examples are given in Ref. [3], Annex I.
4. Exempt quantities are given in Schedule I of Ref. [5].
### TABLE 5. ACTIVITIES CORRESPONDING TO THRESHOLDS OF CATEGORIES

<table>
<thead>
<tr>
<th>Radionuclide</th>
<th>Category 1 1000 × D</th>
<th>Category 2 10 × D</th>
<th>Category 3 D</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(TBq)</td>
<td>(Ci)(^a)</td>
<td>(TBq)</td>
</tr>
<tr>
<td>Cf-252</td>
<td>2.E+01</td>
<td>5.E+02</td>
<td>2.E-01</td>
</tr>
<tr>
<td>Cm-244</td>
<td>5.E+01</td>
<td>1.E+03</td>
<td>5.E-01</td>
</tr>
<tr>
<td>Ir-192</td>
<td>8.E+01</td>
<td>2.E+03</td>
<td>8.E-01</td>
</tr>
<tr>
<td>Se-75</td>
<td>2.E+02</td>
<td>5.E+03</td>
<td>2.E+00</td>
</tr>
<tr>
<td>Tm-170</td>
<td>2.E+04</td>
<td>5.E+05</td>
<td>2.E+02</td>
</tr>
<tr>
<td>Au-198*</td>
<td>2.E+02</td>
<td>5.E+03</td>
<td>2.E+00</td>
</tr>
<tr>
<td>Cd-109*</td>
<td>2.E+04</td>
<td>5.E+05</td>
<td>2.E+02</td>
</tr>
<tr>
<td>Tl-204*</td>
<td>2.E+10</td>
<td>5.E+05</td>
<td>2.E+02</td>
</tr>
</tbody>
</table>

\(a\) 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 sealed radioactive sources with activity levels that would place them within Categories 1, 2 or 3.
In some cases, the radioactive material contained in a radioactive source is nuclear material. The D-values for nuclear material which can be used in a nuclear explosive device are given in Ref. [11] and the same process of categorization using the A/D ratio should be applied in order to categorize them based on the harmful radiological consequences of unauthorized removal for potential offsite exposure or dispersal. There are radionuclides for which D-values are given as “UL” or “unlimited quantity”. This designation is for those radionuclides having very long half-lives and, therefore, low specific activities, very low-energy radiation emissions, or a combination of both. It would therefore be impractical to use such material in a malicious act, and so their categorization for security purposes is unnecessary.

While it may only be possible or appropriate to apply the categorization system described previously to radioactive sources, radioactive waste is another example of radioactive material to which the categorization system may be applied depending on the national context. Radioactive waste refers to radioactive material for which no further use (including reuse or recycling) is foreseen and which is controlled as radioactive waste by the regulatory body.

Like other radioactive material, radioactive waste could cause harmful radiological consequences if used in a malicious act. Radioactive waste is often divided into three general categories for management: high-level waste (HLW) whose definition includes spent nuclear fuel and waste resulting from reprocessing spent nuclear fuel, intermediate-level waste (ILW), and low-level waste (LLW) [29]. With due consideration of the categorization system described in Ref. [29], the assignment of security levels to radioactive waste should follow the steps described in this guidance.

The security levels, goals, and objectives for radioactive waste would be as described in Table 3. Categorization should also take into account radioactive decay and aggregation.

**Radioactive decay**

Because of radioactive decay, the A/D ratio will decline over time. The regulatory body may take this into account in its regulatory practices.

For example, on 1 January 2015 a Co-60 source has an activity level of 56 TBq when it is first used in a device. Calculating the A/D ratio, 56 TBq/0.03 TBq = 1867. So, to start, the source is initially assigned to Category 1.

Co-60 has a half-life of 5.2714 years. After 3 half-lives (approximately 15 years), the Co-60 source has decayed and now has an activity level of 7 TBq so the A/D ratio becomes 7 TBq/0.03 TBq = 233.33, corresponding to Category 2. The regulatory body may choose to require this source to be assigned to Category 1 (based on its original activity level) or to allow this source to be reassigned to Category 2 (based on its current activity level). The regulatory body should clearly indicate it its regulations which approach is followed.
Aggregation of radioactive material

There will be situations in which multiple items containing radioactive material 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). For example, radioactive material should be considered collocated or aggregated if breaching a common physical security barrier (e.g., a locked door at the entrance to a storage room) would allow access to the radioactive material or devices containing the radioactive material.

In such circumstances, the regulatory body should require operators to aggregate the activity of the radioactive material for the purpose of categorization. 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 4, thus allowing the set of different radionuclides to be categorized on the basis of activity. If radioactive material of various radionuclides is aggregated, then the sum of the ratios A/D should be used in determining the category, in accordance with the formula:

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

Where:

- \(A_{i,n}\) = activity of each individual material \(i\) of radionuclide \(n\).
- \(D_n\) = D value for radionuclide \(n\).

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

For example, in a hospital where brachytherapy is performed, 100 Ra-226 sources (0.001 TBq each), 30 Cs-137 sources (0.02 TBq each), and 10 Ir-192 sources (0.22 TBq) are all stored together in a secure room. Because all of these sources may be accessed through a single entry point, they should be aggregated in order to determine the category. To determine the category of these co-located sources, the first step is to determine the category of each set of radioactive sources of the same radionuclide as follows:

For Ra-226: \(\frac{A}{D} = \frac{(100 \times 0.01)}{0.04} = 2.5\), so these are assigned to Category 2.

For Cs-137, \(\frac{A}{D} = \frac{(30 \times 0.02)}{0.1} = 6\) so these are assigned to Category 3.

For Ir-192, \(\frac{A}{D} = \frac{(10 \times 0.22)}{0.08} = 27.5\) so these are assigned to Category 2.

Because various radionuclides are to be stored together in one secure location, they should be aggregated to obtain a total \(\frac{A}{D}\) ratio of \(2.5 + 6 + 27.5 = 36\). As a result, the aggregate of all the radioactive material to be collocated is assigned to Category 2.
### 5.2.2. Assigning security levels

Once radioactive material has been categorized, the next step is to establish a basis for assigning a security level.

As a default arrangement, the regulatory body could use the categories listed in Table 4 or 5 to assign the security level applicable to radioactive material.

On that basis, Category 1 radioactive material should be assigned to Security Level A; Category 2 radioactive material should be assigned to Security Level B; and Category 3 radioactive material should be assigned to Security Level C.

The General Safety Requirements Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards (GSR Part 3, paragraph 3.53 [5]) include general requirements for the control of radioactive sources. Those control measures provide a sufficient level of security for radioactive material in Categories 4 and 5. However, the regulatory body, taking into account relevant threat information, may wish to enhance the security of radioactive material in Categories 4 and 5 in appropriate circumstances.

This approach is summarized in Table 6.

#### TABLE 6. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMON PRACTICES BY CATEGORY

<table>
<thead>
<tr>
<th>Category</th>
<th>A/D</th>
<th>Practice</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A/D ≥ 1000</td>
<td>RTGs, Irradiators, Teletherapy, Fixed multibeam teletherapy (gamma knife)</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>1000 &gt; A/D ≥ 10</td>
<td>Industrial gamma radiography, High/medium dose rate brachytherapy</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>10 &gt; A/D ≥ 1</td>
<td>Fixed industrial gauges that incorporate high activity sources, Well logging gauges</td>
<td>C</td>
</tr>
<tr>
<td>4</td>
<td>1 &gt; A/D ≥ 0.01</td>
<td>Low dose rate brachytherapy (except eye plaques and permanent implants), Industrial gauges that do not incorporate high activity sources, Bone densitometers, Static eliminators</td>
<td>Apply measures as described in GSR Part 3 [5]</td>
</tr>
<tr>
<td>5</td>
<td>0.01 &gt; A/D and A &gt; exempt</td>
<td>Low dose rate brachytherapy eye plaques and permanent implant sources, XRF devices which contain radioactive material, Electron capture devices, Mossbauer spectrometry, Positron emission tomography (PET)</td>
<td></td>
</tr>
</tbody>
</table>
5.2.3. Additional considerations for adjusting security levels

While the assignment of radioactive material to security levels based on category and practice provides a default position, the regulatory body may consider additional specific factors that may lead to adjustment in the security level assigned to particular material on a case by case basis. These factors represent variables that are specific to the radioactive material and the manner and location in which it is used — and these may affect the level of security that is appropriate for given radioactive material or facility. In some cases, these considerations might also lead to the exclusion of certain radioactive material from security requirements altogether.

The regulator may choose to adjust security levels for particular types of radioactive sources or devices as a general matter and include these adjustments in its regulations. For example, it might assign certain types of well logging gauges to Security Level B. Alternatively, the regulatory body could allow the operator to propose an adjustment in the security level of its source, based on specified criteria. In the latter case, the operator would be responsible for seeking approval of the regulatory body for this adjustment.

Mobile, portable and remote sources

Radioactive material used in field applications (e.g., industrial radiography and well logging) are typically contained in relatively small devices designed for portability, are frequently transported between job sites, and are often used in remote locations. The ease of handling and concealment of these devices and their presence in vehicles outside secured facilities make them vulnerable to unauthorized removal.

Special consideration should also be paid to radioactive material in transport that is incidental to use. For example, an industrial radiography device may be transported to various work sites on a daily basis. The transport incidental to use could increase the vulnerability of the radioactive material.

Detailed guidance on security in the transport of radioactive material is given in Ref. [12].

Recognizing that security measures for fixed radioactive material may not be practical for application to radioactive material used in the field, additional or alternative measures should be applied to achieve the security objective. Examples of detection and delay measures for Security Levels B and C are provided in Section 6.

Increased threat level

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

Some fields such as nuclear medicine use radionuclides with short half-lives. Examples of such materials include Tc-99m and F-18 used in radiodiagnosis and I-131 used in radiotherapy. The regulatory body may conclude that such radioactive material is of low security concern because they are likely to decay before they can be used in a malicious act. Further, even if used immediately for malicious purposes, the material would quickly decay below levels which would be harmful. The regulatory body may consider determining a period of time after which radioactive material poses a lower security risk due to radioactive decay (such as ten days or fewer), and can be adequately secured through assignment to a lower security level or through the application of general requirements for the control of radioactive sources.

Long half-life radionuclides

Large amounts of long half-life radionuclides may be found in naturally-occurring radioactive material (NORM), in concentrations which are too small for realizing malicious acts. In other words, the implication of a long half-life is that a large volume is required to obtain an amount of activity attractive to an adversary. Some radionuclides, such as nuclear material as described in Section 5.2.1, may be unattractive to an adversary due to its low specific activity or low-energy radiation emission. For example, 37 GBq of depleted uranium has a mass of approximately 2000 kg. For cases such as these, the regulatory body may choose to reduce the security level since it would not be practicable to use this material in a malicious act.

Ease of handling

Radioactive material that can be easily handled or is easily accessible may be more attractive since the adversary will be less likely to receive a high radiation dose and the radioactive material is more easily moved. An example of this is a radioactive source inside a self-shielded portable device.

Large volume activated or contaminated objects

For various reasons (e.g. the lack of decommissioning funds), some research, industrial and medical institutions may close their facilities without proper transfer of records to the regulatory body. As a consequence, these legacy sites as well as operating facilities may contain activated or contaminated components and structures which are not normally considered subject to specific security requirements during the operating life of a reactor, hot cell, or accelerator. Examples could include various metallic parts from steam generators and dryers, turbine rotors, reactor vessels and vessel heads, reactor coolant pumps, and shielding blocks.

Due to their size and weight, large activated or contaminated components are not easily moved without cranes, rigging, and heavy equipment. In addition, these large components are not easily concealed during loading or when they are in motion, and the amount of time required to remove...
these large components is such that it is reasonable to expect that the operator would detect these
activities. Further, if such a large component were removed, it would be very difficult to use in a
malicious act.

The regulatory body may choose to exempt these components from security requirements or to reduce
their security level.

**Location of radioactive material**

For radioactive material located in a densely populated area where its use in a malicious act may be of
greater security concern, consideration may be given to increasing the assigned security level. One
example is the use of radioactive material for cancer treatment in a hospital located in a largely
populated city. In this case, an increase in the security level assigned to that material may be
warranted. Considerations affecting response times, such as the distance between the facility where
radioactive material is located and the local response force, may also warrant an adjustment of the
assigned security level.

**Radioactive waste**

Security categorization and assignment of security levels of radioactive waste, as described in
Sections 5.2.1 and 5.2.2, remain important steps in the establishment of security measures, taking into
account the ability of States to apply the guidance to radioactive material other than radioactive
sources. However, specific attributes of radioactive waste forms and packages may warrant a
reduction of the assigned security level because these attributes make the material less attractive for
malicious purposes. These attributes include:

(a) Recoverability: Radioactive material may be contained in a solid waste matrix (e.g. a
    concrete block), which makes it very difficult to recover.

(b) Susceptibility to dispersal: Radioactive waste contained within a waste matrix is not readily
    susceptible to dispersal;

(c) Type of waste containers: Certain types of waste containers have additional requirements
    regarding the weight, which make it difficult to transport the radioactive waste because
    they require the use of heavy equipment and significant time.

Depending on the State’s regulatory requirements and infrastructure, radioactive waste may be located
in temporary storage at the operator’s facility, in storage at a designated central storage facility, or in a
disposal facility.

Within a waste disposal facility, there are typically two primary areas: (1) an operations area that is
actively receiving waste and emplacing the waste and (2) a disposal area where waste has been
disposed.
Radioactive waste in the operations area should be protected to the same security level as radioactive material in other locations. In contrast, radioactive waste emplaced in the disposal area often inherently includes one or more physical barriers and may also include limited access points. For example, an adversary attempting to remove radioactive waste from a repository or borehole would be readily detected. Consequently, fewer specific security measures may be required.

The regulatory body may use another approach for assigning a security level to radioactive waste in a disposal area. Radioactive waste located in the disposal area may not be attractive for unauthorized removal by adversaries. In that case, the regulatory body may choose to establish security levels by taking into account the potential for radiological contamination after possible sabotage of a radioactive waste storage facility.

**Other considerations**

Additional factors which may warrant an adjustment of the security level assigned to radioactive material include the perceived economic value of the radioactive material, the equipment it may be inside, and the presence of other hazardous material within the facility where radioactive material is located.

5.3. **STEP 3: IMPLEMENT A REGULATORY APPROACH**

As discussed in Section 3, there are three alternative regulatory approaches that the regulatory body may use for establishing security requirements for radioactive material: prescriptive, performance-based, and combined. The prescriptive approach requires the operator to implement a set of specific required security measures. The performance-based approach requires the operator to design and implement a security system that achieves a required level of performance but allows the operator discretion to identify the particular security measures to be implemented. The combined approach includes elements drawn from both the prescriptive and performance-based approaches.

Regardless of the approach used, regulatory requirements for the security of radioactive material should address each of the following questions:

(a) What is the operator required to protect?
(b) What is the operator required to protect against?
(c) What degree of protection is adequate?
(d) What are the security measures the operator is required to implement?
(e) What are the security management measures the operator is required to implement?

As summarized in Table 7, regulations based on the prescriptive and performance-based approaches address some of these questions in the same way and other questions in different ways. (How
regulations based on the combined approach address these questions will depend on how the regulatory body chooses to combine the two approaches.)

TABLE 7. COMPARISON OF REGULATIONS BASED ON PRESCRIPTIVE AND PERFORMANCE-BASED APPROACHES

<table>
<thead>
<tr>
<th>Question</th>
<th>Prescriptive Approach</th>
<th>Performance-Based Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the operator required to protect?</td>
<td>Specified radioactive material and associated facilities</td>
<td>Specified radioactive material and associated facilities</td>
</tr>
<tr>
<td>What is the operator required to protect against?</td>
<td>The threat, as used by the regulatory body to develop prescriptive security requirements (complete threat information not generally provided to the operator)</td>
<td>The threat, as provided by the regulatory body to the operator for use in designing its security system</td>
</tr>
<tr>
<td>What degree of protection is adequate?</td>
<td>Security Level A, B or C goal and objectives, as applicable to the material</td>
<td>Security Level A, B or C goal and objectives, as applicable to the material</td>
</tr>
<tr>
<td>What are the security measures the operator is required to implement?</td>
<td>The security measures required by the regulatory body based on its determination that they will generally be sufficient to meet the applicable Security Level A, B or C goal and objectives against the threat</td>
<td>The security measures proposed by the operator and accepted by the regulatory body as sufficient to meet the applicable Security Level A, B or C goal and objectives against the threat</td>
</tr>
<tr>
<td>What are the security management measures the operator is required to implement?</td>
<td>The security management measures required by the regulatory body</td>
<td>The security management measures required by the regulatory body</td>
</tr>
</tbody>
</table>

5.3.1. What is the operator required to protect?

Regulations based on either approach should specify the particular radioactive material that the operator is required to protect. Generally, security regulations for radioactive material should cover all radionuclides determined by the regulatory body to represent a security concern based on their potential to cause harmful radiological consequences if used in a malicious act.

As discussed in Section 5.2, the regulatory body may choose to exclude Category 4 and 5 radioactive material from specific security requirements and instead mandate the application of measures described in Ref. [17]. Certain material could be excluded from security requirements based on the additional considerations for assigning security levels discussed in Section 5.

5.3.2. What is the operator required to protect against?

Regulations based on either approach should require the operator to protect against the threat. As discussed in Section 3, to determine the threat, the regulatory body may directly use the national threat assessment or may develop and use a DBT or ATS. The regulatory body should then apply this threat information in a manner consistent with the regulatory approach chosen.
If following the prescriptive approach, the regulatory body should adopt regulations that specify a set of required security measures for detection, delay, and response which the regulatory body has determined will generally be sufficient to meet the applicable security goal and objectives against the threat, if appropriately implemented. In this case, the regulatory body does not generally convey the threat information to operators, except in very general terms.

If following the performance-based approach, the regulatory body should adopt regulations which require the operator to design and implement a security system that is sufficient to meet the applicable security goal and objectives against the threat. In this case, the regulatory body directly shares relevant threat information with operators, subject to stringent information protection requirements.

5.3.3. What degree of protection is adequate?

Regulations based on either approach should require the operator to meet the applicable security goal and objectives. Prescriptive regulations should require the operator to implement required security measures in a manner that meets the applicable security goal and objectives. For example, prescriptive regulations for Security Level A radioactive material should require the operator to implement specified security measures in a manner that provides a very high level of confidence that the security system will prevent unauthorized removal of radioactive material against the threat. Performance-based regulations should require the operator to design and implement a security system that is sufficient to meet the applicable security goal and objectives against the threat.

5.3.4. What are the security measures the operator is required to implement?

Prescriptive regulations require the operator to implement specified security measures. However, because of the wide variation in facilities and activities involving the use or storage of radioactive material, the regulations should give the operator appropriate discretion in implementing the required measures. For example, the regulations might require the operator to implement electronic intrusion detection systems, while leaving the operator flexibility to make such choices as which particular technologies to deploy (e.g., balanced magnetic switch, passive infrared sensors), and how to configure the chosen technologies.

Performance-based regulations require the operator to design and implement a security system consisting of security measures which, implemented together, protect the radioactive material against the threat. In other words, performance-based regulations give the operator the discretion to choose the particular security measures to be implemented, provided the resulting security system achieves the required level of performance.
5.3.5. **What are the security management measures the operator is required to implement?**

Regulations based on either approach should specify security management measures that the operator is required to implement, addressing at least the following topics:

(a) Access control;
(b) Trustworthiness;
(c) Information protection;
(d) Security plan;
(e) Training and qualification;
(f) Accounting;
(g) Inventory;
(h) Security system evaluation; and
(i) Nuclear security event reporting and post-event reporting.

6. **RECOMMENDATIONS ON THE CONTENT OF REGULATIONS**

This section provides recommendations on the content of regulations following the approaches described in Section 5. The recommendations on the prescriptive approach include specific security measures to be included in regulations; the recommendations on the performance-based and combined approaches provide higher level guidance.

6.1. **PRESCRIPTIVE APPROACH**

The regulatory body may choose to establish regulations which specify the security measures that operators are required to have in place in order to meet the security objectives in Table 3. Tables 8, 9 and 10 provide recommended measures for detection, delay and response for Security Levels A, B and C, respectively. These tables apply to radioactive material in use or in storage. Table 9 also includes specific security measures for portable devices used in the field. Table 11 identifies security management measures for all three security levels. The measures are discussed in detail after each corresponding table. This text is intended primarily to clarify the tables for the reader, but could also be incorporated selectively in regulations or guidance.

Regulations that incorporate these security measures should make clear that the operator is required to implement the measures in a manner that meets the applicable security objective. For example, in Table 8, the required delay system of at least two layers of barriers must provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.
6.1. Introduction for Security Level A measures

The goal of Security Level A is to ensure a very high level of confidence that the security system will prevent unauthorized removal of radioactive material. If an attempt at unauthorized access or unauthorized removal is made, detection and assessment needs to occur early enough and delay needs to impede the adversary long enough to enable response personnel to respond in time and with sufficient resources to interrupt the adversary and prevent the radioactive material from being removed. In order to achieve this goal, the following measures should be required.

**Detection**

*Security objective:* Provide immediate detection of unauthorized access to the locations in which radioactive material is present.

Provide immediate detection of attempted unauthorized removal of radioactive material, including removal by an insider.
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 either unauthorized access to the location in which radioactive material is present (see the section on “Delay”) or attempted unauthorized removal of radioactive material. Care should be taken to ensure that such measures cannot be bypassed. For radioactive material in use, such measures should detect unauthorized access to the secured locations where the radioactive material is used. For radioactive material in storage, such measures should detect unauthorized access to the locked room or other location where the radioactive material is stored.

Security objective: Provide immediate assessment of detection.

Security measures: Remote video monitoring or direct observation by operator or response personnel.

Once an 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 location where radioactive material is present, through remote video monitoring (for example, at a central alarm station) or by persons immediately deployed to investigate the cause of the alarm. While video monitoring is an effective assessment measure, it is not a reliable detection measure and should not be used for this purpose.

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

Security measures: Daily verification through physical checks, video monitoring, tamper-indicating devices, radiation monitoring, etc.

Daily verification should consist of measures to ensure that the radioactive material is present and neither the radioactive material nor the device in which it is contained has been tampered with. Such measures could include physical checks that the radioactive material is in place, remote video monitoring, verification of seals or other tamper indicating devices, and measurements of radiation or other physical phenomena that would provide an assurance that the radioactive material is present. For radioactive material in use, verifying that the corresponding device is intact and functional may be sufficient.

Delay

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

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

A balanced system comprising at least two barriers should separate the radioactive material from unauthorized personnel and provide sufficient delay following detection to enable response personnel
to intercede before the adversary can remove the radioactive material or the device in which it is contained. For radioactive material in use, such measures may include a locked device in a secured area to separate the device from unauthorized personnel. For radioactive material in storage, such measures may include a locked and fixed container or a device holding the radioactive material in a locked storage room, thus separating the container from unauthorized personnel.

Response

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable, diverse means of communication such as phones, cell phones, 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. Accordingly, such personnel should be equipped with diverse (at least two) means of communication such as landline telephones, cellular phones, or radios. Where detection and assessment is performed directly by operator personnel, they should be equipped with fixed or mobile duress buttons.

Security objective: Provide for immediate response to assessed alarm with sufficient capability to interrupt and defeat the adversary.

Security measures: Arrangements with a designated response force including provision for sufficient personnel, equipment, and training, documented in a response plan.

In most cases, the operator will not be capable of providing its own response and instead will be reliant on an external response force, typically law enforcement personnel. The State should identify the entity expected to provide such a response within its governmental system. The operator should then be required to establish arrangements with the designated response force to ensure immediate deployment of response personnel without delay in response to an alarm. The regulatory body should facilitate the process of establishing these arrangements.

The planned 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 radioactive material. Adequate means that the response team is of sufficient size and capability to subdue the adversary. The operator’s response arrangements should be documented in the security plan and/or response plan, as further discussed below under Security Management.

6.1.2. Introduction for Security Level B measures

The goal of Security Level B is to ensure a high level of confidence that the security system will prevent unauthorized removal of radioactive material. If an attempt of unauthorized access or
unauthorized removal were to occur, the response needs to be initiated immediately upon detection
and assessment of the intrusion, but relative to Security Level A, the response is not required to arrive
in time to prevent the radioactive material from being removed.

Because Security Level B radioactive material is often used in portable devices deployed in the field,
which cannot be protected in the same manner as radioactive material used or stored in fixed
locations, Table 9 and the accompanying text also include specific security measures that may be
additionally or alternatively required.

In order to achieve the goal for Security Level B, the following measures are recommended.

### TABLE 9. RECOMMENDED DETECTION, DELAY AND RESPONSE MEASURES FOR
SECURITY LEVEL B

*(Goal: High level of confidence that the security system will prevent unauthorized removal of
radioactive material.)*

<table>
<thead>
<tr>
<th>Security function</th>
<th>Security objective</th>
<th>Security measures (radioactive material in use and storage)</th>
<th>Security measures (portable devices containing radioactive material when used in the field)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detection</strong></td>
<td>Provide immediate detection of any unauthorized access to locations where radioactive material is present</td>
<td>Electronic intrusion detection equipment and/or continuous surveillance by operator personnel</td>
<td>Visual observation by two operator personnel</td>
</tr>
<tr>
<td></td>
<td>Provide detection of any attempted unauthorized removal of radioactive material</td>
<td>Tamper detection equipment and/or periodic checks by operator personnel</td>
<td>Visual observation by two operator personnel</td>
</tr>
<tr>
<td></td>
<td>Provide immediate assessment of detection</td>
<td>Remote video monitoring direct observation by operator or response personnel</td>
<td>Observation by operator personnel</td>
</tr>
<tr>
<td></td>
<td>Provide a means to detect loss through verification</td>
<td>Weekly verification through physical checks, tamper detection equipment, etc.</td>
<td>Daily checks after field use</td>
</tr>
<tr>
<td><strong>Delay</strong></td>
<td>Provide delay with high level of confidence that the security system will prevent unauthorized removal</td>
<td>System of two layers of barriers (e.g. walls, cages)</td>
<td>Means of affixing the device to a stationary object if possible</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>Provide immediate communication to response personnel</td>
<td>Rapid, dependable means of communication such as phones, cell phones, radios</td>
<td>Two persons, each equipped with an independent mobile communication device</td>
</tr>
<tr>
<td></td>
<td>Provide immediate initiation of response to interrupt unauthorized removal</td>
<td>Equipment and procedures to immediately initiate response</td>
<td>Advance notification to local response force, and communication after detection</td>
</tr>
</tbody>
</table>
Detection

Security objective: Provide immediate detection of any unauthorized access to locations where radioactive material is present.

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

Portable: Visual observation by two operator personnel

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicates unauthorized access to the location of radioactive material.

Visual observation by two operator personnel achieves immediate detection of unauthorized access to radioactive material contained in portable or mobile devices.

Security objective: Provide detection of any attempted unauthorized removal of radioactive material.

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

Portable: Visual observation by two operator personnel, radiation monitoring of device.

Tamper detection equipment or visual surveillance by operator personnel made during periodic checks indicates attempted unauthorized removal of radioactive material.

Visual observation by two operator personnel or radiation monitoring achieves immediate detection of unauthorized removal of radioactive material contained in portable or mobile devices.

Security objective: Provide immediate assessment of detection.

Security measures: Fixed: Remote video monitoring or direct observation by operator or response personnel.

Portable: Observation by operator personnel

Once an alarm has been triggered, there should be an immediate assessment of the cause of the alarm.

In the case of radioactive material in use and storage, assessment may be performed either through remote video monitoring or through observation by operator or response personnel.

In the case of portable devices, observation by operator personnel is the only feasible means of assessment.

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

Security measures: Fixed: Weekly verification through physical checks, tamper detection equipment, etc.
Portable: Daily checks after field use.

Weekly verification consists of measures to ensure that the radioactive material is present and neither the radioactive material nor the device in which it is contained has been tampered with. Security level A contains some examples of such measures.

For portable devices, radioactive material should be checked daily after use in the field.

**Delay**

*Security objective:* Provide delay to high level of confidence that the security system will prevent unauthorized removal.

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

Portable: Means of affixing the device to a stationary object if possible.

A balanced system of two barriers should separate radioactive material in use or storage from unauthorized personnel.

Portable devices should be affixed to a stationary object in order to delay their removal.

**Response**

*Security objective:* Provide immediate communication to response personnel.

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

Portable: Two persons, each equipped with an independent mobile communication device

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel.

In the case of portable devices used in the field, there should be two operator personnel present at the location, each equipped with mobile communication equipment. The communications equipment should be independent from one another, and tested in advance to ensure coverage.

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

*Security measures:* Fixed: Equipment and procedures to immediately initiate response.

Portable: Advance notification to local response force, and communication after detection

The operator should establish arrangements to ensure immediate deployment of response personnel without delay, in response to an alarm, to interrupt the adversary action.
Operators using portable devices in the field should provide advance notification of their presence to the local response force and communication after detection of an attempted unauthorized removal.

6.1.3. Introduction for Security Level C measures

The goal of Security Level C is to ensure confidence that the security system will prevent unauthorized removal of radioactive material. To the extent appropriate and feasible, the regulatory body may choose to require Security Level B security measures for portable devices containing Security Level C radioactive material when used in the field.

In order to achieve the goal of Security Level C, the following measures are recommended.

<table>
<thead>
<tr>
<th>Security function</th>
<th>Security objective</th>
<th>Security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Provide detection of unauthorized removal of radioactive material</td>
<td>Observation by operator personnel. Tamper detection equipment and/or periodic checks by operator personnel.</td>
</tr>
<tr>
<td></td>
<td>Provide a means to detect loss through verification.</td>
<td>Monthly verification through physical checks, tamper detection equipment.</td>
</tr>
<tr>
<td>Delay</td>
<td>Provide delay with confidence that the security system will prevent unauthorized removal</td>
<td>One barrier (e.g. cage, source housing) or presence of operator personnel.</td>
</tr>
<tr>
<td>Response</td>
<td>Provide prompt communication to response personnel</td>
<td>Rapid, dependable means of communication such as phones, cell phones, radios</td>
</tr>
<tr>
<td></td>
<td>Implement appropriate action in the event of unauthorized removal of radioactive material.</td>
<td>Procedures for identifying necessary actions in accordance with response plan</td>
</tr>
</tbody>
</table>

**Detection**

*Security objective:* Provide detection of unauthorized removal of radioactive material.

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

Operator personnel should be trained to be vigilant in respect of the presence of unauthorized persons.
Operators should verify that the radioactive material is present. Measures could include physical checks that the radioactive material is in place, verification of seals or other tamper detection equipment. Once tamper detection or a physical check indicates that radioactive material 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 verification through physical checks, tamper detection equipment devices, etc.

Monthly verification consists of measures to ensure that the radioactive material is present and neither the radioactive material nor the device in which it is contained has been tampered with. Such measures could include physical checks that the radioactive material is in place, verification of seals or other tamper detection equipment. Security level A contains some examples of such measures.

**Delay**

**Security objective:** Provide delay with confidence that the security system will prevent unauthorized removal

**Security measures:** One barrier (e.g. cage, source housing) or presence of operator personnel.

At least one physical barrier should separate the radioactive material from unauthorized personnel. Such measures may include the source housing or use of the radioactive material in a secured area. The presence of operator personnel may also delay unauthorized access to radioactive material.

**Response**

**Security objective:** Provide prompt communication to response personnel.

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

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, prompt notification should be made to response personnel.

**Security objective:** Implement appropriate action in the event of unauthorized removal of radioactive material.

**Security measures:** Procedures for identifying necessary actions in accordance with response plan.

Regulatory procedures should ensure that any suspected unauthorized removal or loss of radioactive material is assessed and, if confirmed, reported to the appropriate authority without delay. This should be followed by an effort to locate and recover the radioactive material and investigate the circumstances leading to the event.
6.1.4. Introduction for security management measures

For Security Levels A, B, and C, the security objectives and measures for security management are the same; however, a graded approach in implementation of the security measures should be applied. In some cases, the guidance below provides specific recommendations on how the graded approach should be applied; in others, this is left to the discretion of the regulatory body and/or operator.

TABLE 11 RECOMMENDED SECURITY MANAGEMENT MEASURES

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a process for granting individuals authorized unescorted access</td>
<td>Procedures for determining the individuals who need access, verifying that such individuals are trustworthy and reliable and have received necessary training, authorizing access, withdrawing access as appropriate, and maintaining documentation.</td>
</tr>
<tr>
<td>to radioactive material and/or access to sensitive information</td>
<td></td>
</tr>
<tr>
<td>Ensure trustworthiness and reliability of authorized individuals.</td>
<td>Background checks for all personnel authorized for unescorted access to radioactive material and/or for access to sensitive information.</td>
</tr>
<tr>
<td>Provide access controls that effectively restrict unescorted access to</td>
<td>Identification and verification measures</td>
</tr>
<tr>
<td>radioactive material to authorized persons only.</td>
<td></td>
</tr>
<tr>
<td>Identify and protect sensitive information.</td>
<td>Procedures to identify sensitive information and protect it from unauthorized disclosure.</td>
</tr>
<tr>
<td>Provide a security plan.</td>
<td>A security plan which addresses required topics is submitted or made available to the regulatory body and is periodically exercised, evaluated, and revised as appropriate.</td>
</tr>
<tr>
<td>Ensure training and qualification of individuals with security responsibilities.</td>
<td>Assessment of necessary knowledge, skills, and attitudes; provision of corresponding training; procedures for documenting and updating training.</td>
</tr>
<tr>
<td>Conduct accounting and inventory of radioactive material.</td>
<td>Procedures and documentation for verifying radioactive material presence at prescribed intervals; establishment and maintenance of a radioactive material inventory.</td>
</tr>
<tr>
<td>Conduct evaluation for compliance and effectiveness,</td>
<td>Process for verifying that all applicable security requirements are met and for assessing the effectiveness of the security system, employing performance tests as appropriate.</td>
</tr>
<tr>
<td>including performance testing.</td>
<td></td>
</tr>
<tr>
<td>Establish a capability to manage and report security events</td>
<td>Response plan addressing security-related scenarios and procedures for timely reporting of security events</td>
</tr>
</tbody>
</table>

Security objective: Establish a process for granting individuals authorized unescorted access to radioactive material and/or access to sensitive information

Security measures: Procedures for determining the individuals who need access, verifying that such individuals are trustworthy and reliable and have received necessary training, authorizing access, withdrawing access as appropriate, and maintaining documentation.

Operators should be required to limit unescorted access to radioactive material and access to sensitive information to those individuals with a demonstrated need for such access in the performance of their jobs, whose trustworthiness has been verified, and who have received necessary security training. The process for granting access authorization to such individuals should include the following steps:
(a) Determining that an individual needs such access in order to discharge his or her responsibilities;

(b) Obtaining verification that the individual is trustworthy and reliable (see below);

(c) Obtaining verification that the individual has received necessary security training (see below);

(d) Authorizing access based on the above;

(e) Withdrawing access as appropriate as, for example, when an individual’s responsibilities change or when employment is terminated; and

(f) Maintaining current documentation of the results of this process and providing it to those responsible for access control.

**Security objective:** Ensure trustworthiness and reliability of authorized individuals.

**Security measures:** Background checks for all personnel authorized for unescorted access to radioactive material and/or 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 material or, locations where radioactive material is used or stored, or before that person is allowed access to any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive material 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 trustworthiness and reliability of each person. The checks may also include disclosure of criminal conduct. The process should be periodically reviewed and supported through ongoing monitoring 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. Periodic re-checks (e.g. every 5 years) should be conducted.

In many States, the operator will not be authorized to or capable of actually performing background checks and will instead be reliant on law enforcement, the justice ministry or another competent authority to perform such checks at the operator’s request. In such cases, the regulatory body may identify the entity responsible for performing background checks within the State’s governmental system and facilitate the necessary communications between operators and this entity. The results of background checks should be considered sensitive for both security and privacy reasons and therefore should be protected accordingly.

**Security objective:** Provide access controls that effectively restrict unescorted access to radioactive material to authorized persons only.
Security measures: Identification and/or verification measures

Access control is intended to limit access to a location where radioactive material is present 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:

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

Upon verification of a person’s identity and access authorization, the system allows that person to enter the secured area or location of radioactive material, e.g. by opening a lock.

For Security Level A, 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 Security Levels B and C, at least one verification measure should be required.

Security objective: Identify and protect sensitive information.

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

Sensitive information is that which would assist an adversary in overcoming the security system. Such information may include documents, data on computer systems and other media that can be used to identify details of:

(a) The specific location and inventory of radioactive material (sources);
(b) The facility security plan and security arrangements;
(c) Security systems/devices (e.g. intrusion alarms);
(d) Security staffing arrangements and the means of response to events or alarms;
(e) Planned dates, routes and mode of shipment or transfer of radioactive material (sources);
(f) Contingency plans and security response measures.
The operator should be required to establish procedures for identifying such information and protecting it from disclosure during use, storage, and transmission. These procedures should include:

(a) The types of information that needs to be protected;

(b) How it should be marked, controlled and protected, in use, storage, and transmission;

(c) The conditions and manner under which sensitive information may be reproduced, shared among persons with authorized access, and transmitted within and outside the operator’s organization;

(d) Methods for the destruction of documents and other media containing sensitive information;

(e) Arrangements covering management of media containing protected information when they are obsolete or contain information that is no longer considered sensitive.

**Security objective:** Provide a security plan.

**Security measures:** A security plan which addresses required topics; is submitted or made available to the regulatory body; and is exercised, evaluated, and revised as appropriate at least annually.

The operator should be required to develop, implement, exercise, evaluate and revise as necessary a security plan which documents the design, operation and maintenance of the entire security system, as well as the implementation of the other security management elements. The security plan both enables operators to demonstrate to the regulatory body their compliance with security requirements and provides relevant information to facility security personnel for the operation, maintenance and continuous improvement of the security system. For an example of topics that a security plan could be required to address, see Appendix II.

Security plans should be submitted or made available to the regulatory body for review as part of the authorization or inspection process. The operator should be required to exercise, evaluate, and revise the security plan at least annually to ensure that it reflects the current security system and remains effective. Security plans may be different for mobile and portable use sources radioactive material, or for sources radioactive material stored between periods of use. Security plans will contain sensitive information and should be managed accordingly.

The detail contained within a security plan as well as the frequency with which it is exercised, evaluated and revised should be commensurate with the security level of the radioactive material.

**Security objective:** Ensure training and qualification of individuals with security responsibilities.

**Security measures:** Assessment of necessary knowledge, skills and abilities; provision of corresponding training; procedures for documenting and updating training.
The operator should be required to establish requirements for qualification of staff with specific security responsibilities. Such qualification requirements should be based on an assessment of the knowledge, skills, and attitudes necessary to meet the assigned security responsibilities, should generally include (1) minimum educational qualification and previous experience, and may also include (2) minimum physical qualifications, (3) security clearance requirements, and (4) experience or training in the operation of specific security equipment and the implementation of security procedures. The operator should be required to assess each individual against the applicable qualification requirements before assigning that individual to a position with security responsibilities, provide necessary training, periodically re-assess the competence of such staff to perform their assigned duties (re-qualification), and provide re-training as appropriate. All staff should receive general security awareness training.

Training and qualification of all facility personnel should be documented and the records maintained. All training courses and materials should also be regularly reviewed for relevance of content and effectiveness of delivery.

The extent of training and qualification should depend on the knowledge, skills and abilities of security personnel required to meet their responsibilities commensurate with the security level of the operator’s radioactive material.

Security objective: Conduct accounting and inventory of radioactive material.

Security measures: Procedures and documentation for verifying radioactive material presence at prescribed intervals; establishment and maintenance of a radioactive material inventory.

Detection of loss through verification by periodic checking is addressed above under Detection. The accounting element of security management requires the operator to maintain a record indicating the results of each periodic check, including the date and time when the check was performed, the individual who performed the check, and the means used to verify the presence of the radioactive material. If the presence of radioactive material cannot be verified, the operator should be required to report to the regulatory body and/or other government authorities, in a manner and within a time prescribed by regulation and to assist as requested in efforts to locate and recover the radioactive material.

The operator should also be required to establish and maintain an inventory of all radioactive material the operator is authorized to possess.

The operator should be required to adjust the inventory to reflect transfers and receipts within a time prescribed by the regulatory body. Annually, or at another more frequent interval specified by the regulatory body, the operator should verify that the inventory is complete and accurate in all respects, and adjust the inventory to reflect any discrepancies identified. The operator should be required to
report these inventory results to the regulatory body for inclusion in the national registry of radioactively material or radioactive sources.

**Security objective:** Conduct evaluation for compliance and effectiveness, including performance testing.

**Security measures:** Process for verifying that all applicable security requirements are met and for assessing the effectiveness of the security system, employing performance tests as appropriate.

Evaluation is a process by which the operator independently verifies that its facility is in compliance with all applicable security requirements and assesses the effectiveness of its security system to identify any weaknesses that should be corrected and any opportunities for continuous improvement. Evaluation helps ensure that the operator’s security system is reliably operated and maintained, functions as intended, is effective, and meets regulatory requirements.

Performance tests provide one especially useful means of evaluating elements of the security system in order to determine whether they can actually perform as required or produce the desired results. Performance testing, which should be integral to the evaluation process, includes the investigation, measurement, validation or verification of one or more of the following:

(a) People – to verify that personnel understand the security system, follow procedures and use the system properly and as intended;
(b) Procedures – to verify that the procedures produce the desired result and that personnel understand them and properly follow them;
(c) Equipment – to verify that equipment functions as intended and is effective.

The operator should be required to develop and implement an evaluation process that includes performance tests as appropriate.

The comprehensiveness of the evaluation process should be commensurate with the security level of the radioactive material.

**Security objective:** Establish a capability to manage and report security events

**Security measures:** Response plan addressing security-related scenarios and procedures for timely reporting of security events

The operator should be required to develop a response plan for a range of security events, including:

(a) A suspected or threatened malicious act;
(b) A public demonstration which has the potential to threaten the security of sources;
(c) Unauthorized access to a location in which radioactive material is present; and
The operator should develop a response plan addressing these and any other reasonably foreseeable scenarios involving such events and procedures for responding to them. The response plan may be prepared as part of the security plan or as a separate document. External security response forces, as well as emergency response personnel, should be consulted to ensure that their roles and responsibilities are appropriately understood and documented in the response plan, and should be provided with adequate radiation protection. The response plan should be exercised at regular intervals (at least annually) and modified as necessary to address identified weaknesses. The response plan should be coordinated with the radiological emergency plan.

The response plan should include procedures for reporting of security events to the regulatory body, response forces, emergency response organizations, and others as appropriate within a time frame required by the regulatory body commensurate with the significance of the event based on a graded approach. Events to be reported may include:

(a) Discrepancy in accounting data;
(b) Suspected or actual unauthorized removal of a radioactive source;
(c) Unauthorized intrusion into a facility or source storage area;
(d) The discovery of a suspected or actual explosive device in or near a facility or store;
(e) Loss of control over radioactive material;
(f) Unauthorized access to or unauthorized use of radioactive material;
(g) Other malicious acts that threaten authorized activities;
(h) Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of radioactive material;
(i) Failure or loss of security systems that is essential to the protection of radioactive material.

The detail contained within a response plan as well as the frequency with which it is exercised, evaluated and revised should be commensurate with the security level of the radioactive material.

6.2. 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 or ATS where applicable. The regulatory body should further specify a security objective for the classes of radioactive material to which the performance-based approach applies. Generally, such security objectives should be stated in terms of required system effectiveness, as described in Section 4.

A security system that meets applicable security objectives should then be developed by evaluating the security system against the applicable threat information. 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 evaluation (through a vulnerability assessment 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 radioactive material that would be required by the prescriptive approach based on Tables 8-10. While measures addressing the security functions of detection, delay, and response would be included, the particular combination of measures may vary in light of the situation specific analysis conducted in the evaluation of the security system.

The performance based approach should consider the systematic interaction of detection, delay and response in determining overall system effectiveness against the assessed threat. 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.

Regulations using the performance based approach should also include security management measures applicable to the security level of the radioactive material involved, as described in Section 6.1.

6.3. 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 material with lower potential consequences of malicious use, but apply the performance based approach to the radioactive material of highest security concern. For such material, 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 detection, delay, response, and security management.
APPENDIX I. DESCRIPTION OF SECURITY MEASURES

Some of the security measures described below are referenced in Section 5. Others are intended to provide the reader with brief information on additional measures which may be considered.

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 national threat assessment or as defined in the DBT or ATS. Generally, this means the use of high quality, proven equipment and technology which satisfies national or international quality standards.

The security measures are grouped according to security functions as detection, delay and response, and security management.

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. Access control can be supplemented with security examination instruments like package checker, explosion detector, metal detector and radiation gate.

It is also important to limit access to the AACS management computers and software to prevent unauthorized interference with the system database.

CAGES

Metal cages or containers may also be used to segregate and secure radioactive material 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.

FENCES AND GATES

The type of fence used on a perimeter should be appropriate to the threat, the nature of the radioactive material 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.

5 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 (with fence vibration sensors, external motion sensors, infrared and microwave detectors, underground step sensors). The area protection can be supplemented by surface protection by the appropriate combination of opening, glass breaking, glass cutting, wall dismantling and vibration sensors. 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. Video monitoring 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.

16 KEY CONTROL PROCEDURES

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

18 LOCKS, HINGES AND INTERLOCKS FOR DOORS

Locks used for the protection of radioactive material 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 in the measures described for security management. 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. 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.

28 LOCKED, SHIELDED CONTAINERS

Shielding and fixed units containing radioactive material can provide protection, and can delay any attempt to interfere with the radioactive material. However, when operator personnel 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.
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.

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.

TWO PERSON RULE

Certain areas can be accessed only by two persons at the same time.

VIDEO MONITORING

Video monitoring is a useful aid which allows security staff to monitor outer approaches and areas where radioactive material is stored. Cameras can be combined with an intrusion detection system (IDS) to provide event activated camera views along with video capture to allow assessment of an alarm even though the cause of the alarm may no longer be in the immediate vicinity. However, to be fully effective, the performance of video 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. The whole video surveillance and assessment system can consist of analogue and digital (IP-based) cameras, infra reflectors, coaxial and bunched conductor pairs, optical and wireless image transmission devices, and monitors.

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.

WINDOWS AND DOORS

Windows and doors should exhibit sufficient penetration resistance against an intruder. The windows should comply with the same requirements as the doors, which may be ensured by security glass or by a fixed security grill that cannot be disassembled from outside or by an inside security grill that can be
opened, which is fully welded, and made of appropriate steel. The window and door casings and frames should exhibit at least the same resistance as the door and the glass.
APPENDIX II. TOPICS TO BE ADDRESSED IN AN OPERATOR’S SECURITY PLAN

The purpose of a security plan is to describe the security system and procedures that are in place to protect radioactive material in use and storage and associated facilities. The following annotated outline provides high level guidance for drafting a security plan including recommended topics and suggested content that should be considered within each topic. It should be noted that certain sections of the security plan may be developed separately, i.e. the response plan, but should be referenced in the security plan consistent with information security requirements.

1. INTRODUCTION
   
   Objective(s) of the Security Plan
   
   Describe the objectives to be satisfied by the Security Plan, such as documenting the operation of the security system and security management measures in order to meet/demonstrate regulatory requirements/compliance.

   Scope
   
   Briefly describe the areas covered by the Security Plan including its link to other relevant documents or arrangements such as any management, operational, radiation protection or emergency matters.

   Preparation and updating
   
   Describe the process for developing, updating and approving the security plan.

2. FACILITY DESCRIPTION

   This section should describe the radioactive material(s) and their location(s), the level of protection required according to the categorization of the material and the assessed security level, a description of the physical features of the facility and the facilities operations and regulatory requirements.

3. SECURITY MANAGEMENT

   This section should describe the security management measures in place, including:

   (a) Roles and responsibilities
   
   (b) Training and qualification
   
   (c) Access authorization
   
   (d) Trustworthiness
   
   (e) Information protection
   
   (f) Maintenance programme
4. SECURITY SYSTEM

This section should describe how the security system achieves the required level of protection based on a graded approach. The specific measures to be described include:

Threat information

To the extent the threat information is provided by the regulatory body, describe the information in sufficient detail to indicate how the security system is designed to protect against both external and internal threats. Also indicate who is responsible for receiving threat information and how such information is shared with operator personnel who have a need to know.

Security assessment methodology

Describe the process or methodology used to evaluate the security system and assess its vulnerabilities taking into account the threat information provided.

Security system design

Describe how the security system has been designed in order to provide the level of protection required, taking into account the graded approach and the principles of defence in depth and balanced protection. This section should also describe modifications to the security system in the case of increased threat.

Access control

Describe the physical measures for controlling access including how personnel/vehicles are physically controlled at each access control point to limit access only to authorized persons and the specific media used to authenticate the identity of authorized persons/vehicles at access points such as key card, personal identification number, biometric device, or a combination.

Delay, detection and alarm assessment measures

For each of the controlled or secured areas describe the means of detection at each barrier or access point, the barriers (delay measures) used to increase adversary task time relative to response time, the methods of alarm assessment (such as video monitoring, central alarm stations, guard or response forces both internal and external, computer and recording systems).

5. SECURITY PROCEDURES

This section should describe the written procedures for personnel who implement and maintain them, such as routine, off-shift and emergency operations, opening and closing of the facility, key and lock
control, accounting and inventory control, and acceptance and transfer of the radioactive material from one facility to another for example.

6. RESPONSE

This section should describe the response arrangements for all security events, including references to emergency plans and emergency response actions. This section should capture:

- Roles and responsibilities of on-site security or facility personnel during security events, and those of local and national response forces if external response is required;
- Communication methods to be used by response forces when communicating with the alarm monitoring station or facility security personnel; and
- Procedures for reporting security events, including any reporting requirements including arrangements for review of the security system following an event and corrective actions required.

REFERENCES

List any reference documents such as specific regulations, regulatory authorization, operating manuals, organizational policies and manuals etc. that are referred to in the Security Plan or are needed to explain or expand on any details in the Plan.
APPENDIX III. DESCRIPTION OF A VULNERABILITY ASSESSMENT

There are a number of methods that can be used to verify that facilities are in compliance with all applicable security requirements and to assess the effectiveness of their security systems. One such method is a vulnerability assessment (VA), a method of evaluating the effectiveness of a facility’s security system.

Vulnerability can be defined as a weakness or shortcoming within a security system that could be exploited by an adversary. Examples of vulnerability within a facility include:

(a) Ineffective or absent security measures;
(b) Inappropriate administrative controls;
(c) Inadequate communication;
(d) Poor security culture;
(e) Incompatibility with safety systems.

Vulnerability should be assessed against the basic functions of security (detection, delay, response and security management) to ensure that the risks associated with malicious acts against radioactive material and associated facilities, as defined by the State, are managed to an acceptable level.

A VA is a systematic appraisal of the effectiveness of a security system for protection against the threat (or DBT/ATS if one exists). The VA can be specific or general in nature. It can be conducted locally by the operator to demonstrate system effectiveness against the requirements specified by the regulatory body, or to design and/or make modifications to the existing design of the security system. The VA can also be conducted and used by the regulatory body in the development or evaluation of its regulations, or the evaluation of the operator’s security system.

Those conducting the VA should be technical experts familiar with the facility in question, particularly its technical and commercial imperatives, with the appropriate knowledge and skills related to the design and evaluation of security systems.

The VA process comprises three major phases:

(a) Planning the VA – includes determining the scope and objectives of the VA, selecting a methodology, evaluating potential threats and their capabilities, understanding the nature of the facility including the attractiveness of the material and the threat environment, defining the roles and responsibilities of the VA team, determining the resources required and timeframe to complete the assessment, confirming the radioactive material inventory and associated information, taking note of the categorization, form, location and the physical environment.
Conducting the VA - includes defining the requirements of the security system, gathering the data needed to characterize the security system and its components, analyzing the ability of the system to meet the requirements, identifying existing security measures and assessing the expected effectiveness of the security system in protecting against attacks by the assessed threats (and/or DBT/ATS, if one exists), and determining what, if any, additional security measures are necessary to ensure the required level of protection; and

Completing the VA – including the provision of reports outlining the methodology used, the assumptions made, the data collected, the effectiveness of the security system, and recommendations for upgrades if required.
REFERENCES


[19] EUROPOL, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERPOL, WORLD CUSTOMS ORGANIZATION, Combating Illicit Trafficking in Nuclear and Other Radioactive Material, Nuclear Security Series No. 6, IAEA, Vienna (2007)


GLOSSARY

For terms defined in Refs [1] or [3], those definitions apply also to this publication and are not repeated below.

**alternative threat statement.** A description of the motivation, intentions and capabilities of potential adversaries that is established through a less rigorous and formal approach than that used to establish a design basis threat.

**design basis threat.** A comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated.

**disused source.** A radioactive source which is no longer used, and is not intended to be used, for the practice for which an authorization has been granted.

**response 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.

**threat assessment.** An evaluation of the threats — based on available intelligence, law enforcement, and open source information — that describes the motivation, intentions, and capabilities of these threats.

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