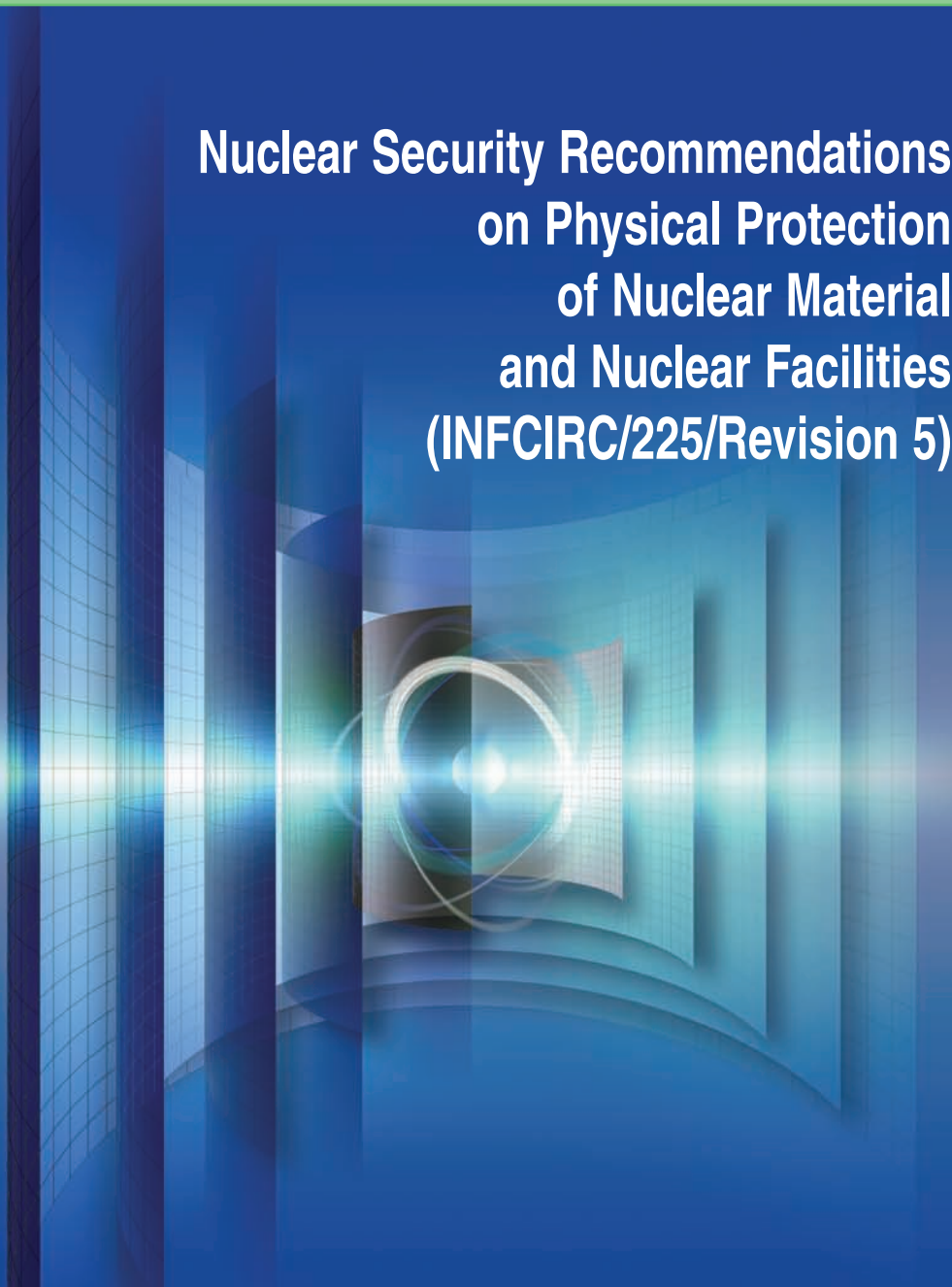
IAEA Nuclear Security Series No. 13

Recommendations

Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)



IAEA
International Atomic Energy Agency

THE IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the **IAEA Nuclear Security Series** of publications. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material, the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- **Recommendations** present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- **Implementing Guides** provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- **Technical Guidance** publications include: **Reference Manuals**, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; **Training Guides**, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and **Service Guides**, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

DRAFTING AND REVIEW

International experts assist the IAEA Secretariat in drafting these publications. For Nuclear Security Fundamentals, Recommendations and Implementing Guides, open-ended technical meeting(s) are held by the IAEA to provide interested Member States and relevant international organizations with an appropriate opportunity to review the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review. This allows Member States an opportunity to fully express their views before the text is published.

Technical Guidance publications are developed in close consultation with international experts. Technical meetings are not required, but may be conducted, where it is considered necessary, to obtain a broad range of views.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns. An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications.

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 13

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)

RECOMMENDATIONS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2011

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria January
2011
STI/PUB/1481
https://doi.org/10.61092/iaea.ko2c-dc4q

IAEA Library Cataloguing in Publication Data

Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/revision 5) : recommendations. — Vienna : International Atomic Energy Agency, 2010.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816-9317 ; no 13)
STI/PUB/1481
ISBN 978–92–0–111110–4
Includes bibliographical references.

1. Nuclear facilities — Safety regulations. 2. Physical protection. 3. Radioactive substances — Law and regulation. I. International Atomic Energy Agency. II. Series.

IAEAL 11–00667

FOREWORD

The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. States have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events. States have agreed to strengthen existing instruments and have established new international legal instruments to enhance nuclear security worldwide. Nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported.

Through its Nuclear Security Programme, the IAEA supports States to establish, maintain and sustain an effective nuclear security regime. The IAEA has adopted a comprehensive approach to nuclear security. This recognizes that an effective national nuclear security regime builds on: the implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of and response to trafficking in such material; national response plans; and contingency measures. With its Nuclear Security Series, the IAEA aims to assist States in implementing and sustaining such a regime in a coherent and integrated manner.

The IAEA Nuclear Security Series comprises Nuclear Security Fundamentals, which include objectives and essential elements of a State's nuclear security regime; Recommendations; Implementing Guides; and Technical Guidance.

Each State carries the full responsibility for nuclear security. Specifically, to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event.

Physical protection against unauthorized removal of nuclear material and against the sabotage of nuclear facilities or transports has long been a matter of national and international concern and cooperation. The international community has agreed to strengthen the Convention on the Physical Protection of Nuclear Material, and it has cooperated with the IAEA in establishing nuclear security guidance.

First published in 1972, the document Recommendations for the Physical Protection of Nuclear Material was prepared by a panel of experts convened by the Director General. After revision, these recommendations were published in 1975 in the INFCIRC series as INFCIRC/225. This document has been favourably received by States and has since become a standard reference. It was revised in 1977, 1989, 1993 and 1998.

In September 2001, the IAEA Board of Governors and the General Conference endorsed 'Physical Protection Objectives and Fundamental Principles' as an important step to strengthen the international physical protection framework. In 2005, awareness started to grow of the need to revise INFCIRC/225/Rev.4 (Corr.) to take into account recent developments and new international legal instruments.

This publication is intended to serve the function of two documents — Revision 5 of INFCIRC/225 and IAEA Nuclear Security Series No. 13 (Recommendations) — on the Physical Protection of Nuclear Material and Nuclear Facilities. It is intended to assist Member States in implementing a comprehensive physical protection regime, including any obligations and commitments they might have with respect to international instruments on nuclear security.

The preparation of this publication in the IAEA Nuclear Security Series has been made possible by the contribution of a large number of experts from Member States. An extensive consultation process with all Member States has included open-ended technical meetings in Vienna, the first in February 2010. The draft was then circulated to all Member States for 120 days to solicit further comments and suggestions. During a final open-ended technical meeting in September 2010, the comments received from Member States were reviewed and consensus was obtained on the final version of this publication.

CONTENTS

1. INTRODUCTION 1

Background (1.1–1.8). 1
Purpose (1.9–1.11) 2
Scope (1.12–1.18) 2
Structure (1.19–1.24) 4

2. OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME (2.1–2.3) 4

3. ELEMENTS OF A STATE'S PHYSICAL PROTECTION REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES 5

State responsibility (3.1–3.2) 5
International transport (3.3–3.7) 6
Assignment of physical protection responsibilities (3.8) 7
Legislative and regulatory framework 7
Legislative and regulatory framework (3.9–3.17) 7
Competent authority (3.18–3.22) 9
Responsibilities of the licence holders (3.23–3.30) 10
International cooperation and assistance (3.31–3.33) 12
Identification and assessment of threats (3.34–3.40) 12
Risk based physical protection system and measures 13
Risk management (3.41–3.42) 13
Graded approach (3.43–3.44) 14
Defence in depth (3.45–3.47) 15
Sustaining the physical protection regime 15
Security culture (3.48–3.51) 15
Quality assurance (3.52) 16
Confidentiality (3.53–3.55) 16
Sustainability programme (3.56–3.57) 17
Planning and preparedness for and response to nuclear security events (3.58–3.62) 17

4. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE 18

General 18
Basis for concern (4.1–4.4) 18
Categorization (4.5–4.8) 19
Requirements for physical protection against unauthorized removal in use and storage 21
General (4.9–4.12) 21
Requirements for Categories I, II and III nuclear material (4.13–4.20) 22
Requirements for Categories I and II nuclear material (4.21–4.35). 22
Requirements for Category I nuclear material (4.36–4.49) 25
Requirements for measures to locate and recover missing or stolen nuclear material 26
Scope and boundary 26
Requirements for the State (4.50–4.56) 27
Requirements for the operator (4.57–4.63) 27

5. REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR FACILITIES AND NUCLEAR MATERIAL IN USE AND STORAGE 29

General (5.1–5.3) 29
Basis for a graded approach for physical protection against sabotage (5.4–5.8) 29
Requirements for the process to design a physical protection system against sabotage (5.9–5.19) 30
Requirements for physical protection against sabotage at nuclear facilities 32
Requirements for high consequence facilities including nuclear power plants (5.20–5.42) 32
Requirements for other nuclear facilities and nuclear material (5.43) 35
Requirements for associated measures to mitigate or minimize the radiological consequences of sabotage 36
Scope and boundary (5.44) 36
Requirements for the State (5.45–5.53) 36
Requirements for the operator (5.54–5.58) 37

6. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT 38

Requirements for physical protection of nuclear material against unauthorized removal during transport (6.1–6.3) 38
General (6.4–6.5) 39
Common requirements for transport of nuclear material (6.6–6.10) 39
Requirements for Categories I, II and III nuclear material (6.11–6.18) 40
Requirements for Categories I and II nuclear material (6.19–6.31) 41
Requirements for Category I nuclear material (6.32–6.43) 43
Requirements for measures to locate and recover nuclear material missing or stolen during transport 45
Scope and boundary (6.44) 45
Requirements for the State (6.45–6.51) 45
Requirements for the carrier (6.52–6.55) 46
Requirements for physical protection of nuclear material against sabotage during transport (6.56–6.59) 46
Requirements for associated measures to mitigate or minimize the radiological consequences of sabotage during transport 47
Scope and boundary (6.60) 47
Requirements for the State (6.61–6.69) 48
Requirements for the carrier (6.70–6.73) 49

DEFINITIONS 51

REFERENCES 57

1. INTRODUCTION

BACKGROUND

1.1. The IAEA has established a Nuclear Security Programme and instituted a series of publications on nuclear security to provide recommendations and guidance that States can use in establishing, implementing and maintaining their national nuclear security regime[1].

1.2. The IAEA Nuclear Security Series framework comprises four tiers of publications: Nuclear Security Fundamentals; Recommendations; Implementing Guides; and Technical Guidance.

1.3. The single top tier publication — Nuclear Security Fundamentals — contains objectives and essential elements of nuclear security and provides the basis for security recommendations.

1.4. The second tier set of Recommendations elaborates on the essential elements of nuclear security and presents the recommended requirements that should be implemented by States for the application of the fundamental principles.

1.5. The third and fourth tiers — Implementing Guides and Technical Guidance — provide more detailed information on implementing the Recommendations using appropriate measures.

1.6. This publication is complementary to and consistent with the Nuclear Security Recommendations publications on:

— Radioactive Material and Associated Facilities [1]; and
— Nuclear and Other Radioactive Material out of Regulatory Control [2].

In order to establish a comprehensive national nuclear security regime, the recommendations contained in all three publications should be implemented.

[1] Historically, the term ‘physical protection’ has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities. As this publication is also Revision 5 of INFCIRC/225, the term physical protection continues to be used throughout the publication.

1.7. The present publication is a Recommendations level document for the physical protection of *nuclear material*[2] and *nuclear facilities*. It is also Revision 5 of INFCIRC/225 [3].

1.8. The present publication will assist Member States to implement a comprehensive *physical protection regime*, including any obligations and commitments they might have as parties to international instruments [4] related to the physical protection of *nuclear material* and *nuclear facilities*, especially the Amendment to the Convention on the Physical Protection of Nuclear Material, of July 2005 [5].

PURPOSE

1.9. This publication provides a set of recommended requirements to achieve the four Physical Protection Objectives (see Section 2) and to apply the 12 Fundamental Principles (see Section 3) that were endorsed by the IAEA Board of the Governors and General Conference in September 2001 [6].

1.10. The purpose of this publication is to provide guidance to States and their *competent authority* on how to develop or enhance, implement and maintain a *physical protection regime* for *nuclear material* and *nuclear facilities*, through the establishment or improvement of their capabilities to implement legislative and regulatory programmes to address the protection of *nuclear material* and *nuclear facilities* in order to reduce the risk of *malicious acts* involving that material or those facilities.

1.11. These recommended requirements are provided for consideration by States and their *competent authority* but are not mandatory upon a State and do not infringe on the sovereign rights of States.

SCOPE

1.12. This publication applies to the physical protection of *nuclear material*, including its physical protection during *transport*, and of *nuclear facilities* against *malicious acts*.

[2] Italicized words in the text represent terms defined in the section on Definitions.

1.13. Three types of risk should be taken into consideration for the protection of *nuclear material* and *nuclear facilities*:

- Risk of *unauthorized removal* with the intent to construct a nuclear explosive device;
- Risk of *unauthorized removal* which could lead to subsequent dispersal;
- Risk of *sabotage*.

1.14. This publication applies to the physical protection of *nuclear material* against *unauthorized removal* with the intent to construct a nuclear explosive device, and to the physical protection of *nuclear facilities* and *nuclear material*, including during transport, against sabotage. Protection requirements against *unauthorized removal* of *nuclear material* for potential subsequent off-site dispersal are provided in IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [1].

1.15. When a facility contains *nuclear material* and other radioactive material, the two sets of protection requirements should be considered and implemented in a manner such that the more stringent requirements for physical protection are applied. This also applies to the *transport* of such material.

1.16. This publication includes actions undertaken to locate and recover *nuclear material* prior to the reporting of lost, missing or stolen *nuclear material* to a *competent authority* (e.g. regulatory body or law enforcement agency) according to national regulations. IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [2], includes actions undertaken to locate and recover material after the reporting.

1.17. This publication does not provide safety requirements. These are contained in the IAEA Safety Standards Series. However, the publication takes safety considerations into account.

1.18. This publication is intended for use in the physical protection of *nuclear material* and *nuclear facilities* used for civil purposes. States may decide whether or not to extend the publication's use to other purposes.

STRUCTURE

1.19. Section 2 provides the objectives of a State's *physical protection regime* for *nuclear material* and *nuclear facilities.*

1.20. Section 3 provides the elements of a State's *physical protection regime* for *nuclear material* and *nuclear facilities.*

1.21. Section 4 provides the requirements for measures against *unauthorized removal* of *nuclear material* in use and storage.

1.22. Section 5 provides the requirements for measures against *sabotage* of *nuclear facilities* and *nuclear material* in use and storage.

1.23. Section 6 provides requirements for measures against *unauthorized removal* and *sabotage* of *nuclear material* during *transport.*

1.24. Italicized words in the text are defined in the Definitions section.

2. OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME

2.1. 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* and other radioactive material. The objectives of the State's *physical protection regime*, which is an essential component of the State's nuclear security regime, should be:

— **To protect against *unauthorized removal.*** Protecting against theft and other unlawful taking of *nuclear material*.
— **To locate and recover missing *nuclear material.*** Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen *nuclear material.*
— **To protect against *sabotage.*** Protecting *nuclear material* and *nuclear facilities* against *sabotage.*
— **To mitigate or minimize effects of *sabotage.*** Mitigating or minimizing the radiological consequences of *sabotage*.

2.2. The State's *physical protection regime* should seek to achieve these objectives through:

— Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;
— Management of an attempted *malicious act* or a *malicious act* by an integrated system of *detection*, delay, and response;
— Mitigation of the consequences of a *malicious act*.

2.3. The objectives mentioned above should be addressed in an integrated and coordinated manner taking into account the different risks covered by nuclear security.

3. ELEMENTS OF A STATE'S PHYSICAL PROTECTION REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES

STATE RESPONSIBILITY

The responsibility for the establishment, implementation and maintenance of a *physical protection regime* within a State rests entirely with that State. (FUNDAMENTAL PRINCIPLE A: Responsibility of the State)

3.1. The State's *physical protection regime* is intended for all *nuclear material* in use and storage and during *transport* and for all *nuclear facilities*. The State should ensure the protection of *nuclear material* and *nuclear facilities* against *unauthorized removal* and against *sabotage*.

3.2. The State's *physical protection regime* should be reviewed and updated regularly to reflect changes in the *threat* and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of *nuclear material* and *nuclear facilities*.

The responsibility of a State for ensuring that *nuclear material* is adequately protected extends to the international *transport* thereof, until that responsibility is properly transferred to another State, as appropriate. (FUNDAMENTAL PRINCIPLE B: Responsibilities during International *Transport*)

3.3. A State's responsibility for physical protection should be determined either by the borders of its sovereign territory or the flag of registration of the transport vessel or aircraft. A State's *physical protection regime* for *nuclear material* in international *transport* should extend to the carriage of material on board ships or aircraft registered to that State while in international waters or airspace and until the receiving State acquires jurisdiction.

3.4. The State's *physical protection regime* should ensure that *nuclear material* is always under the jurisdiction and continuous control of the State and that the point at which responsibility for physical protection is transferred from one State to another and from one carrier to another is clearly defined and implemented by all concerned. International transport operations should be overseen by one or more government organizations having the relevant authority and competence in transport security and/or the appropriate mode of *transport*.

3.5. The shipping State should consider, before allowing international *transport*, if the States involved in the *transport*, including the transit States:

- Are Parties to the Convention on the Physical Protection of Nuclear Material (INFCIRC/274 Rev.1); or
- Have concluded with it a formal agreement which ensures that physical protection arrangements are implemented in accordance with internationally accepted guidelines; or
- Formally declare that their physical protection arrangements are implemented according to internationally accepted guidelines; or
- Have issued licences or other authorizing documents which contain appropriate physical protection provisions for the *transport* of *nuclear material.*

3.6. When international shipments transit the territory of States other than the shipping State and the receiving State, the shipping State should, in advance, identify and inform the other States involved in such transit in order that the

transit States can ensure that the proposed arrangements are in accordance with their national law[3].

3.7. During the international *transport* of Category I *nuclear material*, and possibly other categories of *nuclear material*, especially if accompanied by armed *guards*, the responsibility for *physical protection measures* should be the subject of written arrangements accepted by the States concerned. The relevant *competent authority* of the shipping, receiving, and transit States, and the flag State of the *conveyance* should establish specific measures to ensure the maintenance of communication regarding the continued integrity of the shipment in order to ensure that responsibility for response planning and capabilities is defined and fulfilled. Additionally, any sensitive information shared by States concerned should be protected and the overall arrangements for the shipment should be in accordance with the relevant States' national laws. The point at which responsibility for physical protection is transferred from one State to another should be stated in advance and in sufficient time to enable the relevant State to make adequate physical protection arrangements.

ASSIGNMENT OF PHYSICAL PROTECTION RESPONSIBILITIES

3.8. The State should clearly define and assign physical protection responsibilities within all levels of involved governmental entities including response forces and for *operators* and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State's *physical protection regime*. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the *operator.*

LEGISLATIVE AND REGULATORY FRAMEWORK

Legislative and regulatory framework

The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection

[3] This publication does not affect the exercise of navigation rights and freedoms by ships and aircraft as provided for in international law.

requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of *nuclear facilities* and *transport* to verify compliance with applicable requirements and conditions of the licence or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions. (FUNDAMENTAL PRINCIPLE C: Legislative and Regulatory Framework)

3.9. A State should take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State's *physical protection regime.*

3.10. The State should define requirements — based on the *threat assessment* or *design basis threat* — for the physical protection of *nuclear material* in use, in storage, and during *transport*, and for *nuclear facilities* depending on the associated consequences of either *unauthorized removal* or *sabotage*. The State should ensure that the more stringent requirements for physical protection — either those against *unauthorized removal* or those against *sabotage* — are applied.

3.11. The State's legislation should provide for the comprehensive regulation of physical protection and include a licensing requirement or other procedures to grant authorization. The State should promulgate and review its regulations for the physical protection of *nuclear material* and *nuclear facilities* regularly. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership.

3.12. The State should license activities or grant authorization only when such activities comply with its physical protection regulations. The State should make provisions for a detailed examination, made by the State's *competent authority*, of proposed *physical protection measures* in order to evaluate them for approval of these activities prior to licensing or granting authorization, and whenever a significant change takes place, to ensure continued compliance with physical protection regulations.

3.13. The State should ensure that evaluations include exercises to test the *physical protection system*, including the training and readiness of *guards* and/or *response forces*.

3.14. Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the

trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a *graded approach*. In implementing this policy, the State should ensure that processes are in place to determine the trustworthiness of persons with authorized access to sensitive information or, as applicable, to *nuclear material* or *nuclear facilities*.

3.15. Enforcement of physical protection regulations should be a part of a State's legislative and regulatory framework.

3.16. Sanctions against the *unauthorized removal* and against *sabotage*[4] should be part of the State's legislative or regulatory system.

3.17. The recommended *physical protection measures* in this publication should be additional to, and not a substitute for other measures established for nuclear safety, nuclear material accountancy and control or radiation protection purposes.

Competent authority

The State should establish or designate a *competent authority* which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's *competent authority* and those of any other body in charge of the promotion or utilization of nuclear energy. (FUNDAMENTAL PRINCIPLE D: *Competent Authority*)

3.18. The State's *competent authority* should have a clearly defined legal status and be independent from applicants/*operators*/*shippers*/carriers and have the legal authority to enable it to perform its responsibilities and functions effectively.

3.19. The State's *competent authority* should have access to information from the State's *system for nuclear material accountancy and control*.

[4] The definition of *sabotage* is of a technical nature and does not aim to provide a definition for the purposes of criminal law, such as those provided for in the relevant international instruments or national law of States.

3.20. The State's *competent authority* should be responsible for verifying continued compliance with the physical protection regulations and licence conditions through regular inspections and for ensuring that corrective action is taken, when needed.

3.21. To ensure that *physical protection measures* are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's *competent authority* should ensure that evaluations based on *performance testing* are conducted by *operators* at *nuclear facilities* and, as appropriate, by *shippers* and/or carriers for *transport*. Evaluations should be reviewed by the State's *competent authority*, and should include administrative and technical measures, such as testing of *detection*, assessment, delay and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the *competent authority* should ensure that corrective action is taken by the *operator*, *shipper* and/or carrier.

3.22. The State's *physical protection regime* should include requirements for timely reporting of *nuclear security events* and information which enables the State's *competent authority* to be informed of any changes at *nuclear facilities* or related to *transport* of *nuclear material* that may affect *physical protection measures*.

Responsibilities of the licence holders

The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of *nuclear material* or of *nuclear facilities* rests with the holders of the relevant licences or of other authorizing documents (e.g. *operators* or *shippers*). (FUNDAMENTAL PRINCIPLE E: Responsibility of the Licence Holders)

3.23. In this publication, licence holders are defined as either *operators* or *shippers.*

3.24. The *operator*, *shipper* and carrier should comply with all applicable regulations and requirements established by the State and the *competent authority.*

3.25. The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces*.

3.26. The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority.*

3.27. The *operator* should prepare a security plan as part of its application to obtain a licence. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plan*s. The *competent authority* should review and approve the security plan, the implementation of which should then be part of the licence conditions. The *operator* should implement the approved security plan. The *operator* should review the security plan regularly to ensure it remains up to date with the current operating conditions and the *physical protection system*. The *operator* should submit an amendment to the security plan for prior approval by the *competent authority* before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The *competent authority* should verify the *operator's* compliance with the security plan.

3.28. For a new *nuclear facility*, the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other.

3.29. The *operator* should develop and implement means and procedures for evaluations, including *performance testing*, and maintenance of the *physical protection system.*

3.30. Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority.*

INTERNATIONAL COOPERATION AND ASSISTANCE

3.31. States are encouraged to cooperate and consult, and to exchange information on physical protection techniques and practices, either directly or through the International Atomic Energy Agency and other relevant international organizations.

3.32. States should inform the International Atomic Energy Agency, and other States as applicable, of appropriate points of contact for matters related to the physical protection of *nuclear material* and *nuclear facilities.*

3.33. In the case of *unauthorized removal* or *sabotage* or credible threat thereof, the State should provide appropriate information as soon as possible to other States which appear to it to be concerned, and to inform, where appropriate, the International Atomic Energy Agency and other relevant international organizations.

IDENTIFICATION AND ASSESSMENT OF THREATS

The State's physical protection should be based on the State's current evaluation of the threat. (FUNDAMENTAL PRINCIPLE G: Threat)

3.34. The appropriate State authorities, using various credible information sources, should define the *threat* and associated capabilities in the form of a *threat assessment* and, if appropriate, a *design basis threat*. A *design basis threat* is developed from an evaluation by the State of the threat of *unauthorized removal* and of *sabotage.*

3.35. The States should ensure that the *competent authority* has access to information from other organizations in the State on present and foreseeable threats to nuclear activities.

3.36. When considering the threat, due attention should be paid to *insiders*. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The *physical protection system* should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of *nuclear material* by an *insider.*

3.37. The State's physical protection requirements for *nuclear material* and *nuclear facilities* should be based on a *design basis threat*, specifically for:

— *Unauthorized removal* of Category I *nuclear material* (defined in Section 4),
— *Sabotage* of *nuclear material* and *nuclear facilities* that has potentially high radiological consequences.

The State should decide whether to use a *threat assessment* or *design basis threat* for other *nuclear material* and *nuclear facilities.*

3.38. The State's *competent authority* should require the use of a *threat assessment* and/or a *design basis threat* as a common basis for the design and implementation of the *physical protection system* by the *operator*, *shipper* and carrier. The State should consider whether or not the *threat assessment* and/or *design basis threat* are the same for *nuclear facilities* and for *transport.*

3.39. The State should continuously review the threat and evaluate the implications of any changes in the *threat assessment* or *design basis threat*. The State's *competent authority* should take steps to ensure that any change is appropriately reflected in the regulations and by the *operator's*, *shipper's* and carrier's *physical protection measures*. Recognizing that a revision of the *design basis threat* may take additional time in this process, short term compensatory *physical protection measures* based on the current *threat assessment* should be implemented. The effectiveness of these measures against the current threat should be evaluated. The *design basis threat* should then be reviewed in the light of the revised *threat assessment*.

3.40. The State should give attention to providing protection measures against any airborne threat and against possible *stand-off attacks* specified in the State's *threat assessment* or *design basis threat*.

RISK BASED PHYSICAL PROTECTION SYSTEM AND MEASURES

Risk management

3.41. The State should ensure that the State's *physical protection regime* is capable of establishing and maintaining the risk of *unauthorized removal* and *sabotage* at acceptable levels through risk management. This requires assessing the *threat* and the potential consequences of *malicious acts*, and then developing

a legislative, regulatory and programmatic framework which ensures that appropriate effective *physical protection measures* are put in place.

3.42. Risk can be managed by:

— Reducing the threat. The threat may be reduced, for example, by the deterrence of robust *physical protection measures*, or through the confidentiality of sensitive information;
— Improving the effectiveness of the *physical protection system*. The *physical protection system's* effectiveness may be increased, for example, by implementing *defence in depth* or establishing and maintaining *nuclear security culture*;
— Reducing the potential consequences of *malicious acts* by modifying specific contributing factors, for example, the amount and type of *nuclear material* and the design of the facility.

Graded approach

Physical protection requirements should be based on a *graded approach*, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the *nuclear material* and potential consequences associated with the *unauthorized removal* of *nuclear material* and with the *sabotage* against *nuclear material* or *nuclear facilities*. (FUNDAMENTAL PRINCIPLE H: *Graded Approach*)

3.43. A *graded approach* is used to provide higher levels of protection against events that could result in higher consequences. The State should decide what level of risk is acceptable and what level of protection against the threat should be provided.

3.44. For protection against *unauthorized removal*, the State should regulate the categorization of *nuclear material* in order to ensure an appropriate relationship between the *nuclear material* of concern and the *physical protection measures*. For protection against *sabotage*, the State should establish its threshold(s) of *unacceptable radiological consequences* in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection.

Defence in depth

The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives. (FUNDAMENTAL PRINCIPLE I: *Defence in Depth*)

3.45. State requirements for physical protection should be based on the concept of *defence in depth*. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of *guards* and the performance of their duties) and facility design (including layout).

3.46. The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection.

3.47. *Defence in depth* should take into account the capability of the *physical protection system* and the *system for nuclear material accountancy and control* to protect against *insiders* and external threats.

SUSTAINING THE PHYSICAL PROTECTION REGIME

Security culture

All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization. (FUNDAMENTAL PRINCIPLE F: Security Culture)

3.48. The foundation of *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.

3.49. The four component groups — the State, organizations, managers in organizations and individuals — should work together to establish and maintain an effective *nuclear security culture*.

3.50. The State should promote a *nuclear security culture* and encourage all security organizations to establish and maintain one. A *nuclear security culture* should be pervasive in all elements of the *physical protection regime*.

3.51. All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection.

Quality assurance

A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. (FUNDAMENTAL PRINCIPLE J: Quality Assurance).

3.52. The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements.

Confidentiality

The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of *nuclear material* and *nuclear facilities*. (FUNDAMENTAL PRINCIPLE L: Confidentiality)

3.53. The State should take steps to ensure appropriate protection of specific or detailed information the unauthorized disclosure of which could compromise the physical protection of *nuclear material* and *nuclear facilities*. It should specify what information needs to be protected and how it should be protected, using a *graded approach*.

3.54. Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the

performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected.

3.55. Sanctions against persons violating confidentiality should be part of the State's legislative or regulatory system.

Sustainability programme

3.56. The State should establish a sustainability programme to ensure that its *physical protection regime* is sustained and effective in the long term by committing the necessary resources.

3.57. *Operator*s, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

— Operating procedures (instructions).
— Human resource management and training.
— Equipment updating, maintenance, repair and calibration.
— *Performance testing* and operational monitoring.
— Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
— Resource allocation and operational cost analysis.

PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

***Contingency* (emergency) *plans* to respond to *unauthorized removal* of *nuclear material* or *sabotage* of *nuclear facilities* or *nuclear material*, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned. (Fundamental Principle K: *Contingency Plan*s)**

3.58. The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans*[5] to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration.

3.59. The *operator's contingency plan* should be approved by the State's *competent authority* as a part of the security plan.

3.60. The coordination between the *guards* and *response force*s during a *nuclear security event* should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the *guard*s, *response force*s and other response teams for implementation of the plans.

3.61. Arrangements should be made to ensure that during emergency conditions and exercises, the effectiveness of the *physical protection system* is maintained.

3.62. The *operator* should initiate its *contingency plan* after *detection* and assessment of any *malicious act*.

4. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE

GENERAL

Basis for concern

4.1. An objective of the State's *physical protection regime* is to prevent *unauthorized removal*. An associated objective of the State's *physical protection regime*, also addressed in this section, is to ensure the implementation of rapid and comprehensive measures to locate and recover missing or stolen *nuclear material*. Measures to locate and recover *nuclear material* after the reporting of it

[5] C*ontingency plans* prepared by the *operator* should be consistent with and complementary to the *contingency plan* prepared by the State as mentioned in paras 4.52, 4.53, 5.46 and 5.47.

as lost, missing or stolen to a *competent authority* are addressed in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [2].

4.2. Levels of protection defined in this section are based on categorization of *nuclear material* for use in the construction of a nuclear explosive device. However, *nuclear material* is radioactive material, which has also to be protected against *unauthorized removal* that could have significant consequences if dispersed or used otherwise for a malicious purpose. Protection requirements against *unauthorized removal* of *nuclear material* for potential subsequent off-site radiological dispersal are provided in IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [1].

4.3. These two sets of requirements for protection against *unauthorized removal* should be considered and implemented in a manner such that the more stringent requirements for physical protection are applied.

4.4. When implementing requirements for protection against *unauthorized removal*, the requirements for the protection against *sabotage* addressed in Section 5 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

Categorization

4.5. The primary factor in determining the *physical protection measures* against *unauthorized removal* is the *nuclear material* itself. Table 1 categorizes the different types of *nuclear material* in terms of element, isotope, quantity and irradiation. This categorization is the basis for a *graded approach* for protection against *unauthorized removal* of *nuclear material* that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity.

4.6. According to footnote ‘e’ in Table 1, the protection of *nuclear material* with a radiation level that exceeds 1 Gy/h (100 rad/h) at 1 m unshielded, which is classified as Category I or II before irradiation, may be reduced one category level below that determined by the fissile content of the material. However, if the *threat assessment* or *design basis threat* includes an adversary who is willing to perform a *malicious act*, States should carefully consider whether or not to reduce

TABLE 1. CATEGORIZATION OF NUCLEAR MATERIAL

Material	Form	Category I	Category II	Category III[c]
1. Plutonium [a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (^{235}U)	Unirradiated[b] – Uranium enriched to 20% ^{235}U or more – Uranium enriched to 10% ^{235}U but less than 20% ^{235}U – Uranium enriched above natural, but less than 10% ^{235}U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10kg but more than 1 kg 10 kg or more
3. Uranium-233 (^{233}U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content)[d, e]	

Note: This table is not to be used or interpreted independently of the text of the entire publication.

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h. (100 rad/h) at 1 m unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at one metre unshielded.

the categorization levels of the material on the basis of radiation levels sufficient to incapacitate the adversary before the *malicious act* is completed.

4.7. *Nuclear material*, which is in a form that is no longer usable for any nuclear activity, minimizes environmental dispersal and is practicably irrecoverable, may be protected against *unauthorized removal* in accordance with prudent management practice.

4.8. In determining the levels of physical protection in a facility, which may consist of several buildings, the *operator* may identify, in agreement with the State's *competent authority*, part of the *nuclear facility* which contains *nuclear material* of a different category and which is therefore protected at a different level than the rest of the *nuclear facility.* Conversely, consideration may need to be given to adding together the total amount of *nuclear material* contained in a number of buildings to determine the appropriate protection arrangements for this group of buildings.

REQUIREMENTS FOR PHYSICAL PROTECTION AGAINST UNAUTHORIZED REMOVAL IN USE AND STORAGE

General

4.9. The *physical protection system* of a *nuclear facility* should be integrated and effective against both *sabotage* and *unauthorized removal*.

4.10. Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*.

4.11. The *operator* should assess and manage the physical protection interface with safety and nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

4.12. *Nuclear material* that is required to be protected in accordance with prudent management practice (see Table 1, footnote c and para. 4.7) should be secured against *unauthorized removal* and unauthorized access.

Requirements for Categories I, II and III nuclear material

4.13. In addition to the recommendations in paras 4.9–4.12, the following recommendations apply to Categories I, II and III *nuclear material*.

4.14. *Nuclear material* should be used or stored within at least a *limited access area*.

4.15. Provision should be made for detecting unauthorized intrusion and for appropriate action by sufficient *guards* and/or *response forces* to address a *nuclear security event*.

4.16. Every *nuclear material* handler should be required to conform to procedures for transferring custody of the *nuclear material* to the succeeding handler. Additionally, *nuclear material* handlers should endeavour to ascertain on reporting for duty that no interference with or *unauthorized removal* has taken place.

4.17. Technical means and procedures for access control, such as keys and computerized access lists, should be protected against compromise, e.g. manipulation or falsification.

4.18. For movements of Category III *nuclear material* within a *limited access area*, the *operator* should apply all prudent and necessary *physical protection measures*.

4.19. *Contingency plans* should be prepared to counter *malicious acts* effectively and to provide for appropriate response by *guards* or *response forces*. Such plans should also provide for the training of facility personnel in their actions.

4.20. The State should ensure that *response forces* are familiarized with the site and *nuclear material* locations and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety.

Requirements for Categories I and II nuclear material

4.21. In addition to the recommendations in paras 4.9–4.20, the following recommendations apply to Categories I and II *nuclear material*.

4.22. *Nuclear material* should be used or stored within at least a *protected area*.

4.23. A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion detection and assessment to detect unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken.

4.24. The number of access points into the *protected area* should be kept to the minimum necessary. All points of potential access should be appropriately secured and fitted with alarms.

4.25. Vehicles, persons and packages entering and leaving the *protected area* should be subject to search for *detection* and prevention of unauthorized access and of introduction of prohibited items or removal of *nuclear material*, as appropriate. Entry of vehicles into the *protected area* should be strictly minimized and limited to designated parking areas.

4.26. Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Persons authorized unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors should be escorted by persons authorized unescorted access.

4.27. The identity of authorized persons entering the *protected area* should be verified. Passes or badges should be issued and visibly displayed inside the *protected area*.

4.28. A record should be kept of all persons who have access to or possession of keys, keycards and/or other systems, including computer systems that control access to *nuclear material.*

4.29. On-site movements between two *protected areas* should be treated in compliance with the requirements for *nuclear material* during *transport*, after taking into account existing *physical protection measures* at the facility.

4.30. A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication

with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a threat, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled.

4.31. Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification.

4.32. Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*.

4.33. A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations.

4.34. The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

— Deter an adversary;
— Detect intrusion;
— Inspect visually the physical protection components;
— Supplement the existing *physical protection measures*;
— Provide an initial response.

4.35. Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces* should be conducted regularly to determine reliability and effectiveness against the *threat*. These should be carried out with full cooperation between the *operator* and *response forces.* Significant deficiencies and action taken should be reported as stipulated by the *competent authority.*

Requirements for Category I nuclear material

4.36. In addition to the recommendations in paras 4.9–4.35, the following recommendations apply to Category I *nuclear material*.

4.37. *Nuclear material* should be used or stored within an *inner area*. An *inner area* could also be a *vital area*.

4.38. An *inner area* should provide an additional layer to the *protected area* for *detection*, access control and delay against *unauthorized removal*. *Inner areas* should be appropriately secured and fitted with alarms when unattended.

4.39. *Inner areas* should provide delay against unauthorized access to allow for a timely and appropriate response to an *unauthorized removal*. Delay measures should be designed considering both *insiders'* and external adversaries' capabilities, and should take into account and be balanced for all potential points of intrusion.

4.40. The number of access points to the *inner areas* should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and fitted with alarms.

4.41. Vehicle barriers should be installed at an appropriate distance from the *inner area* to prevent the penetration of unauthorized land and waterborne vehicles specified in the *design basis threat* that could be used by an adversary for committing a *malicious act*. Attention should also be given to providing protection measures against any airborne threat specified in the *design basis threat* for the *operator.*

4.42. Only authorized persons should have access to the *inner area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *inner area* should be kept to the minimum necessary. Persons with authorized access to the *inner area* should be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized unescorted access.

4.43. Vehicles, persons and packages should be subject to search on entering both the *protected* and *inner areas* for *detection* and prevention of unauthorized access and of introduction of prohibited items. Vehicles, persons and packages

leaving the *inner area* should be subject to search for *detection* and prevention of *unauthorized removal*. Instruments for the *detection* of *nuclear material*, metals, and explosives could be used for such searches.

4.44. Private vehicles should be prohibited access to *inner areas*.

4.45. Records should be kept of all persons who access *inner areas* and of all persons who have access to or possession of keys, keycards and/or other systems, including computer systems, that control access to *inner areas.*

4.46. Inside the *inner area*, *nuclear material* should be stored in a hardened room ('strong room') or hardened enclosure that provides an additional layer of *detection* and delay against removing the material. This storage area should be locked and alarms activated except during authorized access to the material. When *nuclear material* is kept in an unoccupied work area outside this storage area, e.g. overnight, equivalent compensatory *physical protection measures* should be established.

4.47. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. a backup alarm station).

4.48. To counter the *insider* threat, whenever an *inner area* is occupied, *detection* of unauthorized action should be achieved by constant surveillance (e.g. the *two person rule*).

4.49. *Guards* and *response forces* should provide an effective and timely response to prevent an adversary from completing the *unauthorized removal.* At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *guards* and the *response forces* can reach this objective.

REQUIREMENTS FOR MEASURES TO LOCATE AND RECOVER MISSING OR STOLEN NUCLEAR MATERIAL

Scope and boundary

This section provides recommendations for the State and *operator* that should participate in a coordinated response for the location and recovery of

missing or stolen *nuclear material*. For the *operator,* these location and recovery measures should include on-site operations and appropriate assistance to the State organizations for off-site operations.

Requirements for the State

4.50. The State should ensure that its *physical protection regime* includes rapid response and comprehensive measures to locate and recover missing or stolen *nuclear material*. These location and recovery measures should include on-site and off-site operations.

4.51. The State should define the roles and responsibilities of appropriate State response organizations and *operators* to locate and to recover any missing or stolen *nuclear material*.

4.52. The State should ensure that *contingency plan*s — including interfaces with safety, as appropriate — are established by *operators* to locate and to recover any missing or stolen *nuclear material*.

4.53. The responsible State organizations should develop *contingency plans* for the rapid location and recovery of *nuclear material* which has been declared missing or stolen from facilities.

4.54. For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations and *operators*. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations.

4.55. The State should ensure that *operators* and appropriate State response organizations conduct exercises to assess and validate the *contingency plans* and also to train the various participants in how to react in such a situation.

4.56. The State should ensure that *contingency plans* for location and recovery are regularly reviewed and updated.

Requirements for the operator

The recommendations for the *operator* are organized by the following process for the location and recovery of missing or stolen *nuclear material*. The steps in this process include *detection*, confirmation, declaration, location, securing and return of the missing or stolen *nuclear material*.

4.57. The *operator* should ensure that any missing or stolen *nuclear material* is detected in a timely manner by means such as the *system for nuclear material accountancy and control* and the *physical protection system* (e.g. periodic inventories, inspections, access control searches, radiation detection screening).

4.58. The *operator* should confirm any missing or stolen *nuclear material* by means of a rapid emergency inventory as soon as possible within the time period specified by the State. A *system for nuclear material accountancy and control* should provide accurate information about the potentially missing *nuclear material* in the facility following a *nuclear security event*.

4.59. The *operator* should notify the *competent authority* and other relevant State organizations of missing or stolen *nuclear material* as specified by the State.

4.60. The *operator's* measures to locate and recover missing or stolen *nuclear material* should be included in its *contingency plan*, and should be regularly tested and evaluated. Appropriate joint exercises should be held with the *competent authority* and other State organizations.

4.61. The *operator* should take all appropriate measures to locate, as soon as possible, any declared missing or stolen *nuclear material* on-site and possibly off-site (in hot pursuit) in accordance with the legal and regulatory framework and the *contingency plan*.

4.62. As soon as possible after the missing or stolen *nuclear material* has been located and identified, the *operator* should, in accordance with the *contingency plan*, secure this material in situ and then return it to an appropriate *nuclear facility* with due authorization from the *competent authority.*

4.63. The *operator* should provide any other necessary assistance to the State organizations to locate and recover *nuclear material* and should cooperate during subsequent investigations and prosecution.

5. REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR FACILITIES AND NUCLEAR MATERIAL IN USE AND STORAGE

GENERAL

5.1. An objective of the State's *physical protection regime* is to protect against *sabotage*. An associated objective of the State's *physical protection regime* also addressed in this section is to ensure the implementation of rapid and comprehensive measures to mitigate or minimize the radiological consequences of *sabotage*, taking emergency plans into account. This section applies to *nuclear facilities*, including nuclear reactors (nuclear power plants and research reactors) and nuclear fuel cycle facilities (including conversion, enrichment, fabrication, reprocessing, and storage facilities). *Nuclear facilities* frequently contain other hazardous material that could have severe non-radiological consequences but this section does not address such material.

5.2. The recommendations for *physical protection measures* in this section are made on the basis of the potential radiological consequences resulting from an act of *sabotage*. The categorization specified in Section 4 is based on the attractiveness of material for the potential construction of a nuclear explosive device, and cannot be directly applied to protection against *sabotage*.

5.3. When implementing requirements for protection against *sabotage*, the requirements for the protection against *unauthorized removal* addressed in Section 4 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

BASIS FOR A GRADED APPROACH FOR PHYSICAL PROTECTION AGAINST SABOTAGE

This section presents the approach to be used to define the *nuclear facilities* and *nuclear material* which require protection against *sabotage*.

5.4. For each *nuclear facility*, an analysis, validated by the *competent authority*, should be performed to determine whether the radioactive inventory has the potential to result in *unacceptable radiological consequences* as determined by

the State, assuming that the *sabotage* acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures.

5.5. On the basis of these analyses, the State should consider the range of radiological consequences that can be associated with all its *nuclear facilities* and should appropriately grade the radiological consequences that exceed its limits for *unacceptable radiological consequences* in order to assign appropriate levels of protection.

5.6. In accordance with the fundamental principle of *graded approach*, the State should define a set of physical protection design objectives and/or measures for each assigned level of protection.

5.7. If the potential radiological consequences of *sabotage* are less severe than the *unacceptable radiological consequences* defined by the State, then the *operator* should still protect safety related equipment and devices by controlling access to them and securing them.

5.8. If the potential radiological consequences of *sabotage* exceed the State's *unacceptable radiological consequences*, then the *operator* should identify equipment, systems or devices, or *nuclear material*, the *sabotage* of which could directly or indirectly lead to this condition as potential *sabotage* targets and protect them in accordance with the following design process (paras 5.9–5.19) and protection requirements (paras 5.20–5.43). The results of safety analysis provide useful input, including target identification and potential radiological consequences, and should be considered during design of the *physical protection system.*

REQUIREMENTS FOR THE PROCESS TO DESIGN A PHYSICAL PROTECTION SYSTEM AGAINST SABOTAGE

This section presents the process to be used to design the *physical protection system* of a *nuclear facility* and *nuclear material* which require protection against *sabotage.*

5.9. Using the *threat assessment* or *design basis threat*, the *operator* — in cooperation with the State's *competent authority* — should define credible scenarios by which adversaries could carry out *sabotage* of *nuclear facilities* and *nuclear material.*

5.10. When defining scenarios, the *operator* should consider the location of the *nuclear facility* and all *nuclear material* and other radioactive material, including radioactive waste, especially those at the same location inside a *nuclear facility.*

5.11. *Sabotage* scenarios should consider external and/or *insider* adversaries who attempt to disperse *nuclear material* or other radioactive material or to damage or interfere with equipment, systems, structures, components or devices, including possible *stand-off attack*, consistent with the State's *threat assessment* or *design basis threat.*

5.12. The *operator* should design a *physical protection system* that is effective against the defined *sabotage* scenarios and complies with the required level of protection for the *nuclear facility* and *nuclear material*.

5.13. The *physical protection system* against *sabotage* should be designed as an element of an integrated system to prevent the potential consequences of *sabotage* by taking into account the robustness of the engineered safety and operational features, and the fire protection, radiation protection and emergency preparedness measures.

5.14. The *physical protection system* should be designed to deny unauthorized access of persons or equipment to the targets, minimize opportunity of *insiders*, and to protect the targets against possible *stand-off attacks* consistent with the State's *threat assessment* or *design basis threat*. The response strategy should include denial of adversary access to the *sabotage* targets or denial of adversary task completion at the *sabotage* targets. Denying access to the targets or denial of adversary task completion is accomplished by the primary physical protection functions of *detection*, delay and response, whereas protecting against *stand-off attacks* involves facility design considerations, barrier design considerations to implement a stand-off distance, and other disruption measures.

5.15. The *operator* should evaluate and the *competent authority* should validate the design of *physical protection system* effectiveness to verify that it complies with the required level of protection for the *nuclear facility* and *nuclear material*.

5.16. If the evaluation of the design of *physical protection system* indicates that it is ineffective, then the *operator* should redesign the *physical protection system* and re-evaluate its effectiveness.

5.17. The *physical protection system* of a *nuclear facility* should be integrated and effective against both *sabotage* and *unauthorized removal*.

5.18. The *operator* should assess and manage the physical protection interface with safety activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

5.19. Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*.

REQUIREMENTS FOR PHYSICAL PROTECTION AGAINST SABOTAGE AT NUCLEAR FACILITIES

This section provides recommendations for physical protection at *nuclear facilities*, including nuclear power plants, the *sabotage* of which could lead to high radiological consequences, and for other *nuclear facilities*.

Requirements for high consequence facilities including nuclear power plants

5.20. *Nuclear material* in an amount which if dispersed could lead to high radiological consequences and a minimum set of equipment, systems or devices needed to prevent high radiological consequences, should be located within one or more *vital areas*, located inside a *protected area*.

5.21. A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed, and appropriate action taken.

5.22. The number of access points into the *protected area* should be kept to the minimum necessary. All points of potential access should be appropriately secured and fitted with alarms.

5.23. Vehicles, persons and packages entering the *protected area* should be subject to search for *detection* and prevention of unauthorized access and of introduction of prohibited items. Instruments for the *detection* of *nuclear material*, metal, and explosives can be used for such searches. Entry of vehicles

into the *protected area* should be strictly minimized and limited to designated parking areas.

5.24. Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Authorized unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined, such as temporary repair, service or construction workers and visitors, should be escorted by persons authorized for unescorted access.

5.25. The identity of authorized persons entering the *protected area* should be verified. Passes or badges should be issued and visibly displayed inside the *protected area*.

5.26. A *vital area* should provide an additional layer to the *protected area* for *detection*, access control and delay. *Vital areas* should be appropriately secured and alarmed when unattended.

5.27. *Vital areas* should provide delay against unauthorized access to allow for a timely and appropriate response to an act of *sabotage* consistent with the *design basis threat.* Delay measures should be designed considering both the *insiders'* and external adversaries' capabilities, and should take into account and be balanced for all potential points of intrusion.

5.28. The number of access points to the *vital areas* should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and fitted with alarms.

5.29. To counter the *insider* threat, whenever persons are present in *vital areas*, provision should be made for timely *detection* of unauthorized action.

5.30. Vehicle barriers should be installed at an appropriate distance from the *vital area* to prevent the penetration of unauthorized land and waterborne vehicles specified in the *design basis threat* that could be used by an adversary for committing a *malicious act*. Attention should be given to providing protection measures against any airborne threat specified in the *design basis threat* for the *operator.*

5.31. Only authorized persons should have access to the *vital area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *vital area* should be kept to the minimum necessary. Authorized access to the *vital area* should be limited to persons whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access.

5.32. Private vehicles should be prohibited from accessing *vital areas*.

5.33. Timely *detection* of tampering or interference with *vital area* equipment, systems or devices should be provided. A timely report should be made to the *competent authority* whenever there is reason to suspect that any malicious activity has occurred.

5.34. During a shutdown/maintenance period, strict access control to *vital areas* should be maintained. Prior to reactor start-up, searches and testing should be conducted to detect any tampering that may have been committed during shutdown/maintenance.

5.35. Records should be kept of all persons who access *vital areas* or have access to or possession of keys, keycards and/or other systems, including computer systems, that control access to *vital areas*.

5.36. A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a threat, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station).

5.37. Alarm equipment, alarm communication paths and the *central alarm station* should be provided with an uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification.

5.38. Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*.

5.39. A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations.

5.40. The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

— Deter an adversary;
— Detect intrusion;
— Inspect visually the physical protection components;
— Supplement the existing *physical protection measures*;
— Provide an initial response.

5.41. Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces*, should be conducted regularly to determine reliability and effectiveness against the *threat*. These should be carried out with full cooperation between the *operator* and *response forces. Performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *response forces* can provide an effective and timely response to prevent *sabotage.* Significant deficiencies and actions taken should be reported as stipulated by the *competent authority.*

5.42. *Contingency plans* should be prepared to effectively counter *malicious acts* and to provide for appropriate response by *guards* or *response forces*. Such plans should also provide for the training of facility personnel in their actions.

Requirements for other nuclear facilities and nuclear material

5.43. *Sabotage* of *nuclear facilities* other than high consequences facilities and of various forms and quantities of other *nuclear material* could also result in radiological consequences to the public. States should determine the level of

protection needed against such *sabotage* depending upon the degree of radiological consequences. Measures specified in paras 5.20–5.42. may be applied in a graded manner as appropriate.

REQUIREMENTS FOR ASSOCIATED MEASURES TO MITIGATE OR MINIMIZE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE

Scope and boundary

5.44. This section provides recommendations for the State and *operator* so that they participate in a coordinated manner to respond to an act of *sabotage* to mitigate or minimize radiological consequences. In the case of *sabotage* or attempted *sabotage* which could affect a *nuclear facility,* two kinds of measures should be taken by the appropriate State response organizations and the *operator.* The *contingency plan* should include measures which focus on preventing further damage, on securing the *nuclear facility* and on protecting emergency equipment and personnel. The emergency plan consists of measures to ensure the mitigation or minimization of the radiological consequences of *sabotage* as well as human errors, equipment failures and natural disasters. These plans should be comprehensive and complementary.

Requirements for the State

5.45. The State should define the roles and responsibilities of appropriate State response organizations and *operators* to prevent further damage, secure the *nuclear facility* and protect emergency equipment and personnel.

5.46. The State's *contingency plan* should complement the *contingency plan* prepared by the *operator.*

5.47. The State should ensure that *contingency plan*s are established by *operators*.

5.48. The *contingency plans* of the State and of the *operators* should include a description of the objectives, policy and concept of operations for the response to *sabotage* or attempted *sabotage*, and of the structure, authorities and responsibilities for a systematic, coordinated and effective response.

5.49. The State should develop arrangements and protocols among appropriate State response organizations and *operators*, for the coordination of measures for

preventing further damage, securing the *nuclear facility* and protecting emergency equipment and personnel. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations.

5.50. The State should ensure that *operators* and appropriate State response organizations conduct exercises to assess and validate the *contingency plan*s prepared by the *operators* and the State organizations, and also to train the various participants on how to react in such a situation.

5.51. The State should ensure that *contingency plans* are regularly reviewed and updated.

5.52. The State should ensure that joint exercises, which simultaneously test emergency and *contingency plan*s and actions, are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems.

5.53. The State should ensure that *response forces* are familiarized with the site and *sabotage* targets and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety.

Requirements for the operator

5.54. The *operator* should establish a *contingency plan*.

5.55. The *operator* should prepare facility personnel to act in full coordination with *guard*s, *response forces*, law enforcement agencies and safety response teams for implementing the *contingency plans*.

5.56. The *operator* should assess, on *detection* of a *malicious act*, whether this act could lead to radiological consequences.

5.57. The *operator* should notify, in a timely manner, the *competent authority*, *response forces* and other relevant State organizations of *sabotage* or attempted *sabotage* as specified in the *contingency plan*.

5.58. Immediately following an act of *sabotage*, the *operator* should take measures to prevent further damage, secure the *nuclear facility* and protect emergency equipment and personnel.

6. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT

The challenges associated with protecting *nuclear material* from *unauthorized removal* and *sabotage* during *transport* are unique compared to when it is held at *nuclear facilities*, and thus require a dedicated approach.

REQUIREMENTS FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST UNAUTHORIZED REMOVAL DURING TRANSPORT

6.1. Levels of protection defined in this section are based on categorization of *nuclear material* for use in the construction of a nuclear explosive device. However, *nuclear material* is radioactive material, which has also to be protected against *unauthorized removal* since it could have significant consequences if dispersed or used otherwise for a malicious purpose. Protection requirements against *unauthorized removal* of *nuclear material* for potential subsequent off-site radiological dispersal are provided in IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [1].

6.2. These two sets of requirements for protection against *unauthorized removal* should be considered and implemented in such a manner that the more stringent requirements for physical protection are applied.

6.3. When implementing requirements for protection against *unauthorized removal*, the requirements for the protection against *sabotage* addressed in paras 6.56–6.59 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

General

6.4. Table 1 in Section 4 is the basis for a *graded approach* to protection against *unauthorized removal* during *transport* of *nuclear material* that could be used in a nuclear explosive device.

6.5. The total amount of *nuclear material* on or in a single *conveyance* should be aggregated to determine a categorization and identify the appropriate protection requirements for the *conveyance*. When different types of *nuclear material* are transported on the same *conveyance*, an appropriate aggregation formula should be used to determine the category of the consignment.

Common requirements for transport of nuclear material

6.6. Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

(a) Minimizing the total time during which the *nuclear material* remains in *transport*.
(b) Minimizing the number and duration of *nuclear material* transfers, i.e. transfer from one *conveyance* to another, transfer to and from temporary storage and temporary storage while awaiting the arrival of a *conveyance*, etc.
(c) Protecting *nuclear material* during *transport* and in temporary storage in a manner consistent with the category of that *nuclear material.*
(d) Avoiding the use of predictable movement schedules by varying times and routes.
(e) Requiring predetermination of the trustworthiness of individuals involved during *transport* of *nuclear material.*
(f) Limiting advance knowledge of transport information to the minimum number of persons necessary.
(g) Using a material transport system with passive and/or active *physical protection measures* appropriate for the *threat assessment* or *design basis threat.*
(h) Using routes which avoid areas of natural disaster, civil disorder or with a known threat.
(i) Ensuring that packages and/or *conveyances* are not left unattended for any longer than is absolutely necessary.

6.7. Appropriate measures, consistent with national requirements and using a *graded approach*, should be taken to protect the confidentiality of information relating to *transport* operations, based on a need to know, including detailed information on the schedule and route. Great restraint should be applied in the use of any special markings on *conveyances*, and also in the use of open channels for transmission of messages concerning shipments of *nuclear material*. When a security related message is transmitted, measures such as coding and appropriate routing should be taken to the extent practicable, and care should be exercised in the handling of such information.

6.8. Before commencing an international shipment, the *shipper* should ensure that the arrangements are in accordance with the physical protection regulations of the receiving State and of other States which are transited.

6.9. Procedures should be established to ensure the security of keys to *conveyances* and security locks commensurate with the categorization of the *nuclear material* being transported.

6.10. If the *conveyance* makes an unexpected extended stop, the *physical protection measures* appropriate for that category of material in storage should be applied to the extent possible and practicable. Physical protection of *nuclear material* in storage incidental to *transport* should be at a level appropriate for the category of the *nuclear material* and provide a level of protection consistent with that required in Section 4 for use and storage.

Requirements for Categories I, II and III nuclear material

6.11. In addition to the recommendations in paras 6.4–6.10, the following recommendations apply to Categories I, II and III *nuclear material.*

6.12. The carrier should give the receiver advance notification of the planned shipment specifying the mode of *transport* (road/rail/water/air), the estimated time of arrival of the shipment and the exact point of handover if this is to be done at some intermediate point before the ultimate destination. This advance notification should be supplied in time to enable the receiver to make adequate physical protection arrangements.

6.13. Physical protection during *transport* should include prior agreement among *shipper*, receiver, and carrier, specifying time, place and procedures for transferring physical protection responsibilities.

6.14. Packages containing *nuclear material* should be carried in closed, locked *conveyances*, compartments or freight containers. However, carriage of packages weighing more than 2000 kg that are locked or sealed may be allowed in open vehicles. Packages should be tied down or attached to the vehicle or freight container and should be secured as appropriate.

6.15. Where practicable, locks and seals should be applied to *conveyances*, compartments or freight containers. If locks and/or seals are used, checks should be made before dispatch and during any intermodal transfer of each *nuclear material* consignment to confirm the integrity of the locks and seals on the package, vehicle, compartment or freight container.

6.16. There should be a detailed search of the *conveyance* to ensure that nothing has been tampered with and that nothing has been affixed to the package or *conveyance* that might compromise the security of the consignment.

6.17. Arrangements should be made to provide sufficient *guards* and/or *response forces* to deal with *nuclear security events* consistent with the category of *nuclear material* being transported and *physical protection measures* should include communication from the *conveyance* capable of summoning appropriate responders.

6.18. The receiver should check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver should notify the *shipper* of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at the destination.

Requirements for Categories I and II nuclear material

6.19. In addition to the recommendations in paras 6.4–6.18, the following recommendations apply to Categories I and II *nuclear material*.

6.20. *Physical protection measures* should include surveillance of the cargo, load compartment or *conveyance*. States are encouraged to use *guards* for such surveillance.

6.21. The receiver should confirm readiness to accept delivery (and handover, if applicable) at the expected time, prior to the commencement of the shipment.

6.22. A transport security plan should be submitted by the *shipper* and/or carrier as appropriate to the *competent authority* for approval. A plan may cover a series of similar movements. This plan should address routing of the shipment, stopping places, destination hand-over arrangements, identification of persons authorized to take delivery, accident procedures, reporting procedures, both routine and emergency, and, as appropriate, *contingency plans*. In choosing the route, the capabilities of the *response forces* should be taken into account. Exercises should be conducted to assess and validate the transport security plan and to train the participants on how to respond to *nuclear security events*.

6.23. Prior to commencing *transport*, the carrier should verify that all *physical protection measures* are in place in accordance with the transport security plan.

6.24. When justified by the State's *threat assessment*, States are encouraged to use armed *guards* for shipments of Category II *nuclear material* to the extent that laws and regulations permit. In those circumstances when *guards* are not armed, compensating measures should be applied.

6.25. *Physical protection measures* should provide sufficient delay in the c*onveyance*, freight container and/or package so that *guards* and/or *response forces* have time for an appropriate response.

6.26. The *conveyance* should be searched immediately prior to loading and shipment. Immediately following completion of the search, the *conveyance* should be placed in a secure area or kept under *guard* surveillance pending its loading and shipment for *transport* and unloading.

6.27. Personnel with physical protection responsibilities should be given written instructions that, when appropriate, have been approved by the *competent authority*, detailing their responsibilities during the *transport*.

6.28. Particular consideration should be given to ensuring confidentiality of information relating to transport operations, including dissemination only to persons with a need to know this information.

6.29. *Physical protection measures* should include provision of continuous two way voice communication between the *conveyance*, any *guards* accompanying the shipment, the designated *response forces* and, where appropriate, the *shipper* and/or receiver.

6.30. Arrangements should be made to provide adequately sized *response forces* to deal with *nuclear security events*. The objective should be the arrival of the *response forces* in time to prevent *unauthorized removal*.

6.31. Depending on the mode of *transport*, the consignment should be shipped by:

— Road, under exclusive use conditions; or
— Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked *conveyance*; or
— Water, in a secure compartment or container which is locked and sealed; or
— Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

While *nuclear material* is on board pending departure, provisions should be made for sufficient *access delay* or compensating measures to meet the *threat assessment* or *design basis threat.*

Requirements for Category I nuclear material

6.32. In addition to the recommendations in paras 6.4–6.31, the following recommendations apply to Category I *nuclear material*.

6.33. The approval by the *competent authority* of the transport security plan should be based on a detailed examination of proposed *physical protection measures*, which should provide sufficient delay so that *guards* and/or *response forces* have time to intervene to prevent *unauthorized removal*. The transport security plan should include the route and arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, *threat assessment* and operating conditions.

6.34. A further authorization by the *competent authority* of the shipment should be required just prior to commencing *transport* and should be conditional on a current *threat assessment* and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment. The consent to a transport operation can include specific limitations and conditions related to the particular circumstances.

6.35. *Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an

appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the *guard* at all times, especially when the *conveyance* is not in motion. States are encouraged to use armed *guards* to the extent that laws and regulations permit. When *guards* are not armed, compensating measures should be applied, such as adding delay barriers to the *conveyance* exterior structure and/or interior cargo area.

6.36. When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, enhanced *physical protection measures* should be applied, such as additional *guards*. The package should be tied down or attached to the *conveyance* or freight container with multiple locking mechanisms that require to be unlocked by two different keys held by two different authorized persons.

6.37. There should be a *transport control centre* for the purpose of keeping track of the current position and security status of the shipment of *nuclear material*, alerting *response forces* in case of an attack and maintaining continuous secure two way voice communication with the shipment and the *response forces*. The *transport control centre* should be protected so that its function can continue in the presence of the *threat.* While the shipment is in progress, the *transport control centre* should be staffed by qualified *shipper* or State designees whose trustworthiness has been predetermined.

6.38. Continuous two way communication systems between the *conveyance*, *transport control centre*, *guards* accompanying the shipment, the designated *response forces*, and where appropriate, the *shipper* and/or receiver should be redundant, diverse and secure.

6.39. The *guards* or *conveyance* crew should be instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of handover of the shipment by secure two way voice communications to the *transport control centre.*

6.40. For shipment by road, designated *conveyance(s)* should be used exclusively for each consignment and should preferably be specially designed to resist attack and equipped with a *conveyance* disabling device. Each *conveyance* should carry a *guard* or crew member in addition to the driver. Each *conveyance* should be accompanied by at least one vehicle with *guards* to conduct a surveillance of the route for any threat indicators and to protect the *conveyance* and initiate an appropriate response.

6.41. During shipment by rail, accompanying *guards* should travel close to the *conveyance* to have proper effective surveillance.

6.42. Shipment by water should be carried out on a dedicated transport vessel.

6.43. Shipment by air should be by aircraft designated for cargo only and on which the *nuclear material* is its sole cargo.

REQUIREMENTS FOR MEASURES TO LOCATE AND RECOVER NUCLEAR MATERIAL MISSING OR STOLEN DURING TRANSPORT

Scope and boundary

6.44. An objective of the State's *physical protection regime*, addressed in this section, is to ensure the implementation of rapid and comprehensive measures to locate and recover missing or stolen *nuclear material*. Measures to locate and recover *nuclear material* after the reporting of it as lost, missing or stolen to a *competent authority* are addressed in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [2].

Requirements for the State

6.45. The State should ensure that its *physical protection regime* includes rapid response and comprehensive measures to locate and recover missing or stolen *nuclear material* during *transport*.

6.46. The State should define the roles and responsibilities of appropriate State response organizations, carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*.

6.47. The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*.

6.48. The responsible State organizations should develop *contingency plans* for the rapid location and recovery of *nuclear material* which has been declared missing or stolen during *transport*.

6.49. For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations.

6.50. The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* and also to train the various participants how to react in such a situation.

6.51. The State should ensure that *contingency plans* for location and recovery operations are regularly reviewed and updated.

Requirements for the carrier

The recommendations for the carrier are organized by the process for the discovery, location, and reporting of lost or stolen *nuclear material*.

6.52. The carrier should be alert during *transport* for any indications that packages have been removed from the *conveyance* or tampered with and should verify during delivery that no packages are missing or have been tampered with.

6.53. The carrier should take immediate action to determine if missing packages are misplaced but still under its control.

6.54. If packages are determined to be missing or have been tampered with, the carrier should immediately report this to relevant authorities and the *shipper.*

6.55. The carrier should provide any requested assistance to the appropriate State organizations to locate and recover *nuclear material* and should cooperate during subsequent investigations and prosecution.

REQUIREMENTS FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST SABOTAGE DURING TRANSPORT

6.56. The recommendations for *physical protection measures* in this section are made on the basis of the potential radiological consequences resulting from an act of *sabotage*. The categorization specified in Section 4 is based on the attractiveness of material for the potential construction of a nuclear explosive

device and cannot be directly applied to protection against *sabotage*. The recommendations should be used by the State, *shippers*, carriers, receivers, *guards* and *response forces* to help ensure protection of *nuclear material* during *transport* against *sabotage*.

6.57. When implementing requirements for protection against *sabotage*, the requirements for the protection against *unauthorized removal* addressed in paras 6.1–6.43 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

6.58. In accordance with the fundamental principle of the *graded approach* to physical protection, the State should define protection requirements that correspond to the level of potential radiological consequences. The safety features of the design of the *transport* package, container and *conveyance* should be taken into account when deciding what additional *physical protection measures* are needed to protect the material against *sabotage*.

6.59. If the current or potential *threat* warrants additional *physical protection measures* to protect against *sabotage*, consideration should be given to:

— Postponing the shipment;
— Rerouting the shipment to avoid high threat areas;
— Enhancing the robustness of the package or the *conveyance*;
— Detailed route surveillance to observe the current environment;
— Providing (additional) *guards*.

REQUIREMENTS FOR ASSOCIATED MEASURES TO MITIGATE OR MINIMIZE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE DURING TRANSPORT

Scope and boundary

6.60. An objective of the State's *physical protection regime* addressed in this section is to ensure the implementation of rapid and comprehensive measures to mitigate or minimize the radiological consequences of *sabotage*, taking into account emergency plans.

Requirements for the State

6.61. The State should define the roles and responsibilities of appropriate State response organizations, carriers and/or other relevant entities to prevent further damage, secure the nuclear *transport* and protect emergency personnel.

6.62. The State should establish a contingency plan for *transport* of *nuclear material*. This plan should complement the *contingency plan* prepared by the carrier and/or other relevant entities.

6.63. The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities.

6.64. The *contingency plans* for *transport* of *nuclear material* of the State, carriers and/or other relevant entities should include a description of the objectives, policy and concept of operations for the response to *sabotage* or attempted *sabotage*, and of the structure, authorities and responsibilities for a systematic, coordinated and effective response.

6.65. The State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities for the coordination of measures for preventing further damage, securing the nuclear *transport* and protecting emergency personnel. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations.

6.66. The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* for *transport* of *nuclear material* and also to train the various participants on how to react in such a situation.

6.67. The State should ensure that *contingency plans* for *transport* of *nuclear material* are regularly reviewed and updated.

6.68. The State should ensure that joint exercises, which simultaneously test emergency and *contingency plans* and actions for *transport* of *nuclear material* are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems.

6.69. The State should ensure that *response forces* are familiarized with typical *transport* operations and *sabotage* targets and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety.

Requirements for the carrier

6.70. The carrier should prepare transport personnel to act in full coordination with *guard*s, *response forces* and law enforcement agencies for implementing the *contingency plan*.

6.71. The *transport control centre* or carrier's management should be informed as soon as an attempt or an act of *sabotage* is detected.

6.72. The carrier should notify, in a timely manner, the *shipper*, the *competent authority*, *response forces* and other relevant State organizations of *sabotage* or attempted *sabotage* as specified in the *contingency plan*.

6.73. Immediately following an act of *sabotage*, the carrier and/or *guards* should take measures to secure the *transport* and minimize the consequences of the act.

DEFINITIONS

Terms used in this publication are defined below and are italicized in the text.

access delay. The element of a *physical protection system* designed to increase adversary penetration time for entry into and/or exit from the *nuclear facility* or *transport*.

central alarm station. An installation which provides for the complete and continuous alarm monitoring, assessment and communication with *guards*, facility management and *response forces*.

competent authority. Governmental organization(s) or institution(s) that has(have) been designated by a State to carry out one or more nuclear security functions.

contingency plan. Predefined sets of actions for response to unauthorized acts indicative of attempted *unauthorized removal* or *sabotage*, including *threats* thereof, designed to effectively counter such acts.

conveyance. For *transport* (a) by road or rail: any vehicle used for carriage of nuclear material cargo; (b) by water: any seagoing vessel or inland waterway craft, or any hold, compartment, or defined deck area of a seagoing vessel or inland waterway craft used for carriage of nuclear material cargo; and (c) by air: any aircraft used for carriage of nuclear material cargo.

defence in depth. The combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised.

design basis threat. The attributes and characteristics of potential *insider* and/or external adversaries, who might attempt *unauthorized removal* or *sabotage*, against which a *physical protection system* is designed and evaluated.

detection. A process in a *physical protection system* that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm.

force-on-force exercise. A *performance test* of the *physical protection system* that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the *threat* or the *design basis threat*.

graded approach. The application of *physical protection measures* proportional to the potential consequences of a *malicious act.*

guard. A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or *transport*, controlling access and/or providing initial response.

inner area. An area with additional protection measures inside a *protected area*, where Category I *nuclear material* is used and/or stored.

insider. One or more individuals with authorized access to *nuclear facilities* or *nuclear material* in *transport* who could attempt *unauthorized removal* or *sabotage*, or who could aid an external adversary to do so.

limited access area. Designated area containing a *nuclear facility* and *nuclear material* to which access is limited and controlled for physical protection purposes.

malicious act. An act or attempt of *unauthorized removal* or *sabotage*.

nuclear facility. A facility (including associated buildings and equipment) in which *nuclear material* is produced, processed, used, handled, stored or disposed of and for which a specific licence is required.

nuclear material. Material listed in Table 1, in Section 4 of this publication, including the material listed in its footnotes.

nuclear security culture. The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serves as means to support, enhance and sustain nuclear security.

nuclear security event. An event that is assessed as having implications for physical protection.

operator. Any person, organization, or government entity licensed or authorized to undertake the operation of a *nuclear facility.*

performance testing. Testing of the *physical protection measures* and the *physical protection system* to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements.

physical barrier. A fence, wall or similar impediment which provides *access delay* and complements access control.

physical protection measures. The personnel, procedures, and equipment that constitute a *physical protection system*.

physical protection regime. A State's regime including:

—The legislative and regulatory framework governing the physical protection of *nuclear material* and *nuclear facilities*;
—The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;
—Facility and transport *physical protection systems.*

physical protection system. An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*.

protected area. Area inside a *limited access area* containing Category I or II *nuclear material* and/or *sabotage* targets surrounded by a *physical barrier* with additional *physical protection measures*.

response forces. Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted *unauthorized removal* or an act of *sabotage*.

sabotage. Any deliberate act directed against a *nuclear facility* or *nuclear material* in use, storage or *transport* which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.

shipper. Any person, organization or government that prepares or offers a consignment of *nuclear material* for *transport* (i.e. the consignor).

stand-off attack. An attack, executed at a distance from the target *nuclear facility* or *transport*, which does not require adversary hands-on access to the target, or require the adversary to overcome the *physical protection system.*

system for nuclear material accountancy and control. An integrated set of measures designed to provide information on, control of, and assurance of the presence of *nuclear material*, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of *nuclear material*, and ensure the integrity of those systems and measures.

threat. A person or group of persons with motivation, intention and capability to commit a *malicious act.*

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

transport. International or domestic carriage of *nuclear material* by any means of transportation, beginning with the departure from a *nuclear facility* of the *shipper* and ending with the arrival at a *nuclear facility* of the receiver.

transport control centre. A facility which provides for the continuous monitoring of a *transport* conveyance location and security status and for communication with the *transport* conveyance, *shipper/*receiver, carrier and, when appropriate, its *guards* and the *response forces*.

two person rule. A procedure that requires at least two authorized and knowledgeable persons to be present to verify that activities involving *nuclear material* and *nuclear facilities* are authorized in order to detect access or actions that are unauthorized.

unacceptable radiological consequences. A level of radiological consequences, established by the State, above which the implementation of *physical protection measures* is warranted.

unauthorized removal. The theft or other unlawful taking of *nuclear material*.

vital area. Area inside a *protected area* containing equipment, systems or devices, or *nuclear material*, the *sabotage* of which could directly or indirectly lead to high radiological consequences.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[3] Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, IAEA, Vienna (2011).

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

[6] Measures to Improve the Security of Nuclear Materials and other Radioactive Materials, GC(45)/INF/14, IAEA, Vienna (14 September 2001).

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

IAEA Nuclear Security Series No. 15

STI/PUB/1488 (42 pp.; 2011)
978–92–0–112210–0 Price: €23.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES

IAEA Nuclear Security Series No. 14

STI/PUB/1487 (35 pp.; 2011)
ISBN 978–92–0–112110–3 Price: €22.00

INTERNATIONAL LEGAL FRAMEWORK FOR NUCLEAR SECURITY

IAEA International Law Series No. 4

STI/PUB/1486 (30 pp.; 2011)
ISBN 978–92–0–111810–3 Price: €26.00

THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES

INFCIRC/225/Rev.4 (Corrected) Price: Cost free

This publication, Revision 5 of *Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225), is intended to provide guidance to States and their competent authority on how to develop or enhance, implement, and maintain a physical protection regime for nuclear material and nuclear facilities, through the establishment or improvement of their capabilities to implement legislative and regulatory programmes. The goal is to address the protection of nuclear material and nuclear facilities in order to reduce the risk of malicious acts involving such material or facilities.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–111110–4
ISSN 1816–9317