

IAEA Nuclear Security Series No. 26-G

Implementing Guide

**Security of
Nuclear Material
in Transport**



IAEA

International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss 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.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

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. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

SECURITY OF
NUCLEAR MATERIAL
IN TRANSPORT

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

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

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. 26-G

SECURITY OF
NUCLEAR MATERIAL
IN TRANSPORT

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

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>

© IAEA, 2015

Printed by the IAEA in Austria

October 2015

STI/PUB/1686

IAEA Library Cataloguing in Publication Data

Security of nuclear material in transport : implementing guide. — Vienna : International Atomic Energy Agency, 2015.

p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816-9317 ; no. 26-G)
STI/PUB/1686

ISBN 978-92-0-102015-4

Includes bibliographical references.

1. Radioactive substances — Transportation. 2. Radioactive substances — Safety measures. 3. Nuclear industry — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL

15-00997

FOREWORD

by Yukiya Amano
Director General

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

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

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

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

CONTENTS

| | | |
|----|---|----|
| 1. | INTRODUCTION | 1 |
| | Background (1.1–1.3) | 1 |
| | Objective (1.4) | 3 |
| | Scope (1.5–1.9) | 3 |
| | Structure (1.10) | 4 |
| 2. | OBJECTIVES OF A STATE’S PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL (2.1–2.4) | 5 |
| 3. | ELEMENTS OF A STATE’S PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL (3.1) | 6 |
| | State responsibility (3.2–3.7) | 7 |
| | International transport (3.8–3.20) | 8 |
| | Assignment of physical protection responsibilities (3.21–3.24) | 11 |
| | Legislative and regulatory framework (3.25–3.42) | 11 |
| | Identification and assessment of threats (3.43–3.56) | 16 |
| | Sustaining the physical protection regime (3.57–3.69) | 21 |
| | Planning and preparedness for and response to nuclear security events (3.70–3.77) | 25 |
| 4. | CHARACTERIZATION OF NUCLEAR MATERIAL FOR THE APPLICATION OF SECURITY IN TRANSPORT (4.1–4.3) | 26 |
| | Nuclear material categorization and aggregation (4.4–4.17) | 27 |
| | Potential additional physical protection measures for Category III and less than Category III nuclear material (4.18–4.22) | 33 |
| | Potential radiological consequences of sabotage (4.23–4.25) | 35 |
| | Identification of applicable physical protection measures (4.26–4.27) | 35 |

| | | |
|----|--|----|
| 5. | DEVELOPMENT AND IMPLEMENTATION OF ELEMENTS OF A PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL (5.1–5.2) | 36 |
| | Specifying and applying physical protection (5.3–5.13) | 37 |
| | Responsibilities for physical protection in transport (5.14–5.23) | 39 |
| | Key functions of a physical protection system (5.24–5.30) | 42 |
| | Developing the transport security plan (5.31–5.39) | 43 |
| 6. | MEASURES AGAINST THE UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN TRANSPORT (6.1–6.5) | 46 |
| | Mode independent provisions (6.6–6.70) | 47 |
| | Mode specific provisions (6.71–6.108) | 62 |
| | Additional physical protection measures based on potential radiological consequences (6.109–6.112) | 70 |
| 7. | MEASURES TO LOCATE AND RECOVER NUCLEAR MATERIAL MISSING OR STOLEN DURING TRANSPORT | 71 |
| | States' responsibilities (7.1–7.9) | 71 |
| | Carriers' responsibilities (7.10–7.13) | 73 |
| 8. | MEASURES FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST SABOTAGE DURING TRANSPORT (8.1) | 73 |
| | General approach for designing measures against sabotage during transport (8.2–8.24) | 74 |
| | Defining physical protection measures against sabotage (8.25–8.31) | 79 |
| 9. | MEASURES TO MITIGATE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE DURING TRANSPORT (9.1–9.3) | 80 |
| | Responsibilities (9.4–9.6) | 80 |
| | Planning (9.7–9.9) | 81 |
| | Carrier actions (9.10–9.12) | 82 |

APPENDIX I: THE TRANSPORT SECURITY PLAN 83

APPENDIX II: THE VULNERABILITY ASSESSMENT..... 94

REFERENCES 99

GLOSSARY..... 101

1. INTRODUCTION

BACKGROUND

1.1. Threats to nuclear security could include criminals acquiring and using nuclear material to build nuclear explosive devices or radioactive material to cause harm to individuals or the environment through the construction of radiological dispersal devices or radiation exposure devices. Such threats could also include the dispersal of radioactive material through the sabotage of facilities in which radioactive material is used or stored, or during transport. The consequences of such malicious uses of nuclear and radioactive material could be severe, particularly in the case of a nuclear explosive device.

1.2. The Convention on the Physical Protection of Nuclear Material (CPPNM) [1], for which the IAEA is the depositary, provides a worldwide framework for ensuring the physical protection¹ of nuclear material used for peaceful purposes while in international nuclear transport. It also applies, with certain exceptions, to nuclear material while in domestic use, storage and transport. The CPPNM obliges each State Party, inter alia:

- (a) To take appropriate steps to ensure that during international nuclear transport, nuclear material within its territory or on board a ship or aircraft under its jurisdiction, in so far as such ship or aircraft is engaged in the transport to or from that State, is protected;
- (b) To cooperate in the recovery and protection of nuclear material in the case of theft, robbery or any other unlawful taking of or credible threat thereof;

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. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13 [2] uses the term ‘physical protection’ throughout (including the term ‘physical protection regime’ for those aspects of a nuclear security regime related to the unauthorized removal and sabotage of nuclear material and nuclear facilities). To aid understanding of this publication as guidance on the implementation of Ref. [2], the term ‘physical protection’ is used to refer to those aspects of nuclear security relating to measures against unauthorized removal or sabotage of nuclear material and nuclear facilities. For example, a State’s ‘physical protection regime’ comprises those parts of its nuclear security regime that relate to such measures.

- (c) To make certain offences, such as theft or robbery involving nuclear material, punishable by appropriate penalties, which take into account their grave nature.

The scope of the CPPNM, however, does not fully address the protection of nuclear material in domestic use, storage and transport, or of nuclear facilities. The 2005 Amendment to the Convention on the Physical Protection of Nuclear Material [3], *inter alia*, extends the scope of the CPPNM to also cover nuclear facilities and nuclear material in domestic use, storage and transport used for peaceful purposes as well as sabotage thereof. Pursuant to the amended CPPNM, States Parties would be obliged, *inter alia* [3]:

- (i) To establish, implement and maintain a physical protection regime applicable to nuclear material and nuclear facilities under their jurisdiction, including: an appropriate legislative and regulatory framework for physical protection; a competent authority responsible for its implementation; and other administrative measures necessary for the physical protection of such material (and facilities).
- (ii) To consult and cooperate with other States Parties and other relevant organizations, with a view to obtaining guidance on the design, maintenance and improvement of national systems of physical protection for nuclear material in international transport.
- (iii) To take appropriate steps to ensure that during international nuclear transport, nuclear material under their jurisdiction is protected at prescribed levels.

1.3. To support the application of the CPPNM and its Amendment by a State, shippers, carriers and receivers, recommendations have been developed and issued in Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13 [2]. Reference [2] sets out fundamental principles and recommended requirements to provide the essential elements of a State's nuclear security regime (as defined in the Nuclear Security Fundamentals [4]) relating to the physical protection of nuclear material and nuclear facilities. Although Ref. [2] provides recommendations on the physical protection of nuclear material in storage, use and transport, it does not give detailed guidance on implementation and compliance responsibilities for the transport of nuclear material. This Implementing Guide is therefore intended to assist States' competent authorities and shippers or carriers to fulfil their physical protection responsibilities in the transport of nuclear material. Where the term

‘shipper or carrier’ is used in this publication, it refers to the entity to which any specific physical protection responsibility related to transport is assigned.

OBJECTIVE

1.4. The objective of this publication is to provide guidance to States and their competent authorities on how to implement and maintain a physical protection regime for the transport of nuclear material. This publication may also be useful to shippers or carriers in the design and implementation of their physical protection systems. This publication builds upon the recommendations in Ref. [2] and provides additional guidance on how to implement these recommendations in practice.

SCOPE

1.5. This publication applies to the physical protection of nuclear material in transport. It provides guidance for protection against three types of malicious act:

- (a) Unauthorized removal with the intent to construct a nuclear explosive device;
- (b) Unauthorized removal which could lead to subsequent dispersal;
- (c) Sabotage.

1.6. This publication is intended to provide guidance for nuclear security in the transport of nuclear material from one facility to another (i.e. off-site). However, the recommendations may be applied to on-site transport, as the State deems necessary.

1.7. This publication also describes nuclear security measures to locate and recover nuclear material immediately after recognizing the material is missing, prior to the reporting of lost, missing or stolen nuclear material. Detailed guidance on this aspect can be found in the Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15 [5]. This Implementing Guide does not address emergency preparedness and response aspects of a nuclear security event involving nuclear material in transport. These aspects are covered in other IAEA publications [6–8].

1.8. Another Implementing Guide, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9 [9], addresses security in the transport of radioactive material and establishes “security levels for the protection of radioactive material in transport and appropriate security measures commensurate with the potential radiological consequences that could result from malicious use of radioactive material.” Reference [9] applies to the “transport of all packages containing nuclear material...and radioactive material that may pose a significant radiological hazard to individuals, society and the environment as a consequence of a malicious act.” Therefore, it addresses only the concerns regarding potential radiological consequences should nuclear or other radioactive material be used in a radiological dispersal device. It does not address concerns regarding the use of nuclear material in a nuclear explosive device. Thus, the guidance provided in Ref. [9] is complementary to that provided in this publication on the nuclear security needed for the transport of nuclear material.

1.9. It is recognized that nuclear security and safety considerations for the transport of nuclear material should work in concert to enable compliance with IAEA Safety Standards Series No. SSR-6, Regulations for the Safe Transport of Radioactive Material (2012 Edition) [10] (hereinafter referred to as the ‘IAEA Transport Regulations’) as well as with international obligations for nuclear security of nuclear material and other relevant IAEA safety standards and nuclear security guidance. Other regulations, standards, codes and guides developed for safety purposes may also apply, and can influence the design and implementation of a shipper’s or carrier’s transport security system. Thus, such regulations, standards, codes and guides should be considered by a State for ensuring adequate levels of nuclear security.

STRUCTURE

1.10. This publication follows the structure of Ref. [2]. Section 2 summarizes the objectives arising from Ref. [2] that relate to a State developing the transport elements of its physical protection regime. Section 3 addresses the responsibilities of the State in establishing and maintaining a physical protection regime that includes those elements necessary for ensuring the physical protection of nuclear material in transport. Section 4 elaborates on the categorization of nuclear material for the application of nuclear security in transport. Section 5 elaborates on the responsibilities of the shipper or carrier in developing and implementing a physical protection system for specific shipments of nuclear material, and in establishing, implementing and maintaining a physical protection system for those shipments,

with an emphasis on the development and application of transport security plans (TSPs). Section 6 elaborates on measures to be taken to protect against the unauthorized removal of nuclear material in transport by listing specific baseline guidance for the application of the prescriptive approach of developing a physical protection system. This baseline guidance follows a graded approach according to the categorization of the nuclear material, outlining mode independent, mode specific and international provisions. Section 7 elaborates on measures to be taken to locate and recover nuclear material missing or stolen during transport. Section 8 addresses measures for the physical protection of nuclear material against sabotage during transport. Section 9 addresses measures to mitigate or minimize the radiological consequences of sabotage during transport. Appendix I outlines the structure of an example TSP. Appendix II provides a summary of a vulnerability assessment.

2. OBJECTIVES OF A STATE’S PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL

2.1. Paragraph 2.1 of Ref. [2] states that:

“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. Paragraph 2.2 of Ref. [2] states:

“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. Paragraph 2.3 of Ref. [2] states that:

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

2.4. Each of these objectives applies to the physical protection of nuclear material in transport. This publication addresses actions which can be taken towards meeting these objectives in transport.

3. ELEMENTS OF A STATE’S PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL

3.1. This section sets forth guidance that will assist a State and its competent authorities in establishing and maintaining the physical protection regime as applied to transport. This section:

- (a) Lists each fundamental principle and other key elements of the State’s nuclear security regime, as presented in Ref. [2];
- (b) Considers the implementation of each principle as applied to transport activities.

STATE RESPONSIBILITY

Fundamental Principle A: Responsibility of the State

“The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State” [2].

3.2. Each State should take appropriate steps to ensure that an effective physical protection regime exists within the State, including those elements of the regime relating to the physical protection of nuclear material in transport (para. 3.1 of Ref. [2]).

3.3. Each State has a responsibility to regulate the physical protection of nuclear material in transport in order to protect the material from unauthorized removal and to protect public health and safety from radiological consequences that could result from sabotage of the material while in transport. Responsibility rests entirely with the State for ensuring that its physical protection regime provides effective protection of material under its jurisdiction until responsibility is properly transferred to a transit or receiving State.

Establishing transport elements of a physical protection regime

3.4. The State should ensure that a comprehensive physical protection regime is established, implemented and maintained that includes:

- (a) The legislative and regulatory framework governing the physical protection of the nuclear material in transport;
- (b) The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework in relation to the transport of nuclear material;
- (c) Physical protection systems specific to transport.

Physical protection in transport should be an integral part of the State’s overall physical protection regime for nuclear material (para. 3.1 of Ref. [2]).

3.5. A State should have an adequate and supportive legislative base and governmental organization. This should include competent authorities designated by the State that are responsible for enforcing the State’s requirements, including a regulatory body for nuclear security.

3.6. The elements of the State's physical protection regime relating to the transport of nuclear material should be reviewed and updated regularly by the competent authorities to reflect changes in the threat and advances made in physical protection approaches and technologies.

3.7. The State should ensure that the competent authorities, including the regulatory body, are effectively independent of organizations promoting or using nuclear technology. This means that organizational units that are responsible for licensing and supervisory activities are protected by regulatory or organizational means from any undue influence on the execution of their tasks from other units or bodies. If the transport elements of the State's physical protection regime are divided between two or more authorities, arrangements should be made for overall coordination. Clear lines of responsibility should be established and recorded between the relevant entities so that continuous protection of the material is ensured.

INTERNATIONAL TRANSPORT

Fundamental Principle B: Responsibilities during International Transport

“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” [2].

3.8. A State's physical protection regime should ensure adequate physical protection of nuclear material, not only within its own borders but also on ships and aircraft registered to that State engaged in transport to or from that State while in international waters or airspace and until responsibility is transferred to another State (para. 3.3 of Ref. [2]).

State assignment of responsibilities for the international transport of nuclear material

3.9. When international transport of nuclear material takes place, there is also a need for effective international cooperation, including liaison with relevant international organizations, until responsibility is transferred to another State. Only by ensuring continuity of physical protection responsibilities during the entire transport operation can a State fulfil this principle (paras 3.3 and 3.4 of Ref. [2]).

3.10. States involved in international transport should ensure that coordination with transit or receiving States is undertaken so that continuous and adequate protection of the material is ensured as responsibility for the nuclear material is transferred from one State to another (paras 3.3 and 3.4 of Ref. [2]).

3.11. International shipments may involve land transport by road or rail, transport by aircraft or ship, transfers between different forms of transport, transit through multiple States and in-transit storage. In all cases, the relevant competent authorities should make sure that the physical protection of the material is ensured throughout the shipment and that the point of transfer of responsibilities to another State is clearly defined. For land transports, the point of transfer of responsibilities to another State will be determined by the border between the States concerned. For maritime shipments, the point of transfer of responsibility to the receiving State should be clearly defined. In cases where a ship with nuclear material is transiting through other States' territorial waters, the responsibilities for physical protection should be clearly defined until the ship resumes passage in international waters. For air transport, notwithstanding the flag State of the aircraft, the point of transfer of responsibility will normally be the point at which the material is loaded or unloaded, depending on the agreement between the States.

3.12. The shipping State should ensure that all involved States are prepared to accept these responsibilities before a shipment is authorized. Reference [2] provides several ways in which a State can ensure that involved States, including transit States, are prepared to accept these responsibilities, as follows:

- (a) Verifying that all States are party to the CPPNM;
- (b) Concluding formal agreements to ensure physical protection will be implemented in accordance with international agreements;
- (c) Obtaining formal declarations that physical protection will be provided in accordance with internationally accepted guidelines;
- (d) Ensuring that licences or authorizations containing appropriate physical protection arrangements have been issued (paras 3.5 and 3.7 of Ref. [2]).

3.13. In international transport of Category I nuclear material, the responsibility for physical protection measures should be subject to a written agreement between the States concerned. Such agreements may also be reached for international transports of Category II and III nuclear material.

3.14. In addition, when international shipments of nuclear material are to pass through 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 and obtain their cooperation and assistance for adequate physical protection measures and for response actions in the territory of such States in case of any attempted unauthorized removal from, or sabotage of, an international shipment. Such arrangements for advance notification among States involved should not affect the exercise of navigation rights and freedom by ships and aircraft as provided for in international law (paras 3.6 and 3.7, and footnote 3 of para. 3.6 of Ref. [2]).

3.15. International shipments of Category III nuclear material are normally made by normal commercial transport shipping companies. The shipper or carrier should determine whether the transit or receiving States have notification or other requirements applicable to the transit, or receipt of Category III nuclear material, and comply with any such requirements.

3.16. In the case of international shipments of Category I or II nuclear material, the shipping and receiving States should establish specific measures to ensure the maintenance of communication regarding the continued integrity of the shipment and to ensure that responsibility for response planning and capabilities is defined and fulfilled.

3.17. When armed guards are used to protect a shipment, it is particularly important to have written agreements that are accepted by all States involved in advance of the shipment. Agreements regarding armed guards and communications may need to be concluded at the State level, since commercial organizations are unlikely to be able to make such agreements. Shippers and States should ensure that they plan sufficient time for State to State agreements for the shipment to be concluded.

3.18. These agreements should clearly define responsibility for response planning and identify appropriate response capabilities required for the shipment. Since information on these arrangements is particularly sensitive, all involved States should ensure protection of the information.

3.19. Arrangements for the shipment, including the points at which responsibility is transferred from one State to another, should be concluded in sufficient time before the shipment so that all affected States can complete their physical protection arrangements (para. 3.7 of Ref. [2]).

3.20. Where agreements and arrangements involve the exchange of sensitive information, arrangements should be made to accomplish this while protecting the information appropriately. This may involve the shipping, receiving and transit States.

ASSIGNMENT OF PHYSICAL PROTECTION RESPONSIBILITIES

3.21. A State's physical protection regime should assign all necessary physical protection responsibilities, including those for response forces, at all levels of government (para. 3.8 of Ref. [2]).

3.22. The State should ensure that all physical protection responsibilities throughout the transport of nuclear material are clearly assigned to the shipper, the carrier, the receiver or another relevant entity (para. 3.8 of Ref. [2]).

3.23. States may hold the shipper responsible for physical protection during transport and, in such cases, will require that the shipper either conduct the transport operation itself or use a carrier that implements physical protection measures under the direction of the shipper. Alternatively, the State may assign the physical protection responsibilities to authorized carriers, and the operator or shipper will then rely on the carrier's physical protection system (para. 3.8 of Ref. [2]).

3.24. The State's physical protection regime should also assign responsibility for response to any nuclear security events during transport, which may include several levels of government. The regime should clearly indicate responsibilities for response, including those of the shipper and/or carrier during transport, for each category of nuclear material (para. 3.8 of Ref. [2]).

LEGISLATIVE AND REGULATORY FRAMEWORK

Fundamental Principle C: 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 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” [2].

3.25. The State should ensure that a comprehensive legislative and regulatory framework is established with the jurisdiction and responsibility to ensure the physical protection of shipments of nuclear material. The legislative and regulatory framework for physical protection in transport should be an integral part of the State’s overall physical protection regime (para. 3.9 of Ref. [2]).

3.26. The legislative and regulatory framework for the transport of nuclear material should include the designation, funding and staffing of competent authorities for transport security, with authority and responsibility for ensuring that the State’s requirements for physical protection in the transport of nuclear material are understood and adhered to by shippers and carriers under the State’s jurisdiction.

3.27. Enforcement of physical protection regulations is a necessary part of a State’s physical protection regime. Thus, for the transport of nuclear material, the State should assign the power to initiate legal proceedings or to impose sanctions in accordance with the law, where such sanctions may involve suspension of licences and/or other penalties (para. 3.15 of Ref. [2]).

Fundamental Principle D: 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” [2].

3.28. The functions assigned to competent authorities for transport security should include:

- (a) Licensing or authorizing shippers and carriers to transport nuclear material.
- (b) Performing inspections of transports of nuclear material to ensure that shipments are undertaken in full compliance with the applicable requirements and conditions established by the competent authorities.

- (c) Defining requirements or objectives for physical protection in transport based on the threat assessment or design basis threat (DBT). These requirements or objectives should take into account the need for physical protection against the unauthorized removal of nuclear material and against sabotage, and the competent authorities should ensure that the more stringent requirements or objectives are applied.
- (d) Specifying requirements for, and when applicable approving, transport security plans (TSPs).
- (e) Promulgating comprehensive regulations for physical protection in transport. These regulations should be periodically reviewed for adequacy.
- (f) Ensuring the performance of evaluations, consistent with a graded approach and including exercises where appropriate, to test the physical protection systems for transport, and the training and readiness of guards and/or response forces.
- (g) Defining which transport related information should be considered as sensitive and ensuring that its confidentiality is protected accordingly.
- (h) Ensuring that trustworthiness determinations are made, using a graded approach, for all personnel that have physical protection responsibilities during transport or access to sensitive information.
- (i) Establishing a means to enforce applicable requirements and conditions (paras 3.10–3.14 of Ref. [2]).

3.29. The State's competent authorities should have a clearly defined legal status, independence from operators, shippers and carriers, and have the legal authority and capabilities to perform their responsibilities and functions effectively (para. 3.18 of Ref. [2]).

Competent authorities' role in requiring transport security plans for nuclear material

3.30. The competent authorities need to effectively communicate to shippers or carriers those requirements that they must satisfy in order to design and implement a physical protection system that will be acceptable under the State's physical protection regime. An important element will be the design of, and compliance with, a TSP, appropriate to the category of nuclear material being transported. The competent authorities should issue instructions to shippers or carriers specifying requirements for a TSP to ensure that all elements of a State's physical protection requirements are met.

3.31. The competent authorities should ensure there is clear responsibility for, and ownership of, the TSP. For Category I and II nuclear material, the TSP should address routing of the shipment, stopping places, handover arrangements at the destination, identification of persons authorized to take delivery, accident procedures, routine and emergency reporting procedures, and, as appropriate, contingency plans, including their coordination with emergency plans. The competent authorities may also require that shipments of Category III and less than Category III nuclear material be subject to a similar or modified process, depending on the State's requirements or assessment of the threat. For example, the competent authorities may require that shipments of lower category material be transported in accordance with plans, but that these plans may be generic and reflect previously approved measures.

3.32. Information required in a TSP under these provisions may be incorporated into plans developed for other purposes, such as contingency plans. However, TSPs will frequently contain sensitive information that should be restricted to those who need to know it for the performance of their duties. Such information should not be included in plans developed for other purposes if this would result in it being disseminated more widely.

3.33. The TSP should specify how the shipper or carrier will report nuclear security events and other information that may affect the performance of the plan to the competent authorities. Examples of such information that should be reported include:

- (a) Suspicious behaviour of individuals that might indicate preparations for a malicious act, such as photographing or filming conveyances or transport casks;
- (b) Demonstrations along transport routes;
- (c) Major road construction work along transport routes.

Role of competent authorities in establishing an inspection regime

3.34. The State's competent authorities are responsible for verifying, through regular inspections, compliance with physical protection regulations and applicable licence conditions throughout all transport of nuclear material and for ensuring that corrective actions are taken, when needed.

3.35. The objective of an inspection regime is to verify the compliance of measures actually in place with regulatory requirements and applicable licence conditions, including compliance with the TSP.

3.36. Inspections should be performed by qualified and suitably trained personnel designated by the State, and may include both announced and unannounced inspections. The State may specify requirements for inspectors, such as necessary qualifications or training. Inspections should take place during transport operations and at the premises of shippers or carriers. This will ensure that all physical protection measures, including technical, procedural and administrative measures, are reviewed and evaluated. Inspections conducted during transport operations should not unduly impede or affect the normal progress of the shipment.

3.37. Unannounced inspections may need particularly careful consideration. For example, an unannounced inspection during transport operations involving armed guards or response forces might be mistaken for an attack. In such cases, it would be preferable to use an announced inspection or force-on-force exercise.

3.38. If inspections discover non-compliance or other issues, the findings should be graded based on their potential consequences, and acted upon commensurately with this grading. Inspectors should define, in consultation with the shipper or carrier, deadlines for the completion of corrective actions, and should monitor progress and follow-up actions to ensure they have been completed as required.

3.39. The number and nature of inspections conducted should be determined based on the category of nuclear material, its relative attractiveness to potential adversaries, the number of shipments the shipper or carrier has completed and their general level of compliance, the threat assessment and any other relevant factors. However, all shippers or carriers should be inspected on a suitable periodic basis to ensure continued compliance.

Fundamental Principle E: Responsibility 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)” [2].

3.40. The State should ensure that shippers or carriers are assigned the primary responsibility for implementing an effective physical protection system for the transport of nuclear material. In fulfilling this responsibility, the shippers or carriers should comply fully with the regulations and other requirements issued by the State (para. 3.24 of Ref. [2]).

3.41. A shipper may have the prime responsibility for ensuring that various elements of the physical protection system for the transport of nuclear material are appropriately developed and implemented. Specifically, the responsibility for planning the security of the shipment(s) rests with the shipper, acting in conjunction with any related shipping facility and any carriers to be used, and the receiving facility (the receiver). The extent to which the shipper relies on the carrier for performance of nuclear security functions will vary depending on the nature of the contractual arrangement between the shipper and carrier and national regulations. Alternatively, a State may choose to license and impose regulatory requirements upon carriers of nuclear material outside of licensed nuclear facilities. When authorized by the State, the receiver may fulfil some of the roles of the shipper.

3.42. If deficiencies are discovered in the physical protection system that prevent it from providing the required level of protection, the shipper or carrier is responsible for taking immediate compensatory measures, such as providing additional guards, barriers and surveillance, to ensure appropriate protection of the shipment. These measures should be closely coordinated with other entities involved, such as the competent authorities and response forces. The shipper or carrier should then implement corrective actions and have these actions approved by the competent authorities (para. 3.30 of Ref. [2]).

IDENTIFICATION AND ASSESSMENT OF THREATS

Fundamental Principle G: Threat

“The State’s physical protection should be based on the State’s current evaluation of the threat” [2].

3.43. The State should assess the present and foreseeable threats related to the transport of nuclear material and ensure that the evaluation remains adequate and current. The State’s threat assessment should consider all pertinent factors relating to existing or potential threats that could attempt a malicious act. The State may communicate the results of the threat assessment to the shipper

or carrier as a basis for the design of physical protection systems and measures. Alternatively, the State may base its regulatory framework on its evaluation of the threat and require specific physical protection measures appropriate to counter the threat. The State may choose to issue a DBT for transport, specifically for the unauthorized removal of Category I nuclear material.

Approaches for specifying required physical protection provisions: Applying Fundamental Principle G

3.44. Fundamental Principle G specifies that the State should base its physical protection regime on a current evaluation of the threat. Different States will have different capabilities to identify and evaluate threats. Some States have sophisticated security and intelligence capabilities that can assist the competent authorities in understanding the nature and extent of threats, including those that might be directed towards nuclear material in transport. In other cases, general information about the national threat (such as areas and nature of civil unrest or criminal activity) will need to be understood and evaluated to identify the potential threats within a State. In all cases, this should be done cooperatively among the State agencies that have responsibilities for understanding and responding to threats (including, as appropriate, intelligence, police and military authorities). Based on this evaluation of the threat, the competent authorities can make decisions on how to effectively counter the threat with physical protection in transport (paras 3.34 and 3.35 of Ref. [2]).

3.45. Three different approaches for specifying requirements to address the assessed threat are described in Section 5. These are the prescriptive approach, the performance based approach and the combined approach. For each category of nuclear material shipped, the physical protection measures applied should either comply with the administrative and technical requirements specified in the State's regulatory framework (if the State uses the prescriptive approach or some variants of the combined approach) or should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment (if the State uses the performance based approach or other variants of the combined approach).

3.46. Following a graded approach, the State may choose to apply one of these approaches to all three categories of nuclear material, specify that different approaches be used for different categories of material or allow more than one approach to be used for a given category of nuclear material. For example, the State may choose to specify that the prescriptive approach be used for all shipments of nuclear material. In this case, the State should ensure that the

prescribed physical protection measures are sufficient to counter the assessed threat or DBT. Alternatively, the State may choose to specify that:

- (a) The prescriptive approach be used for shipments of Category III nuclear material;
- (b) Either the prescriptive or the combined approach be used for shipments of Category II nuclear material;
- (c) Only the performance based approach be used for shipments of Category I nuclear material.

Review of threat

3.47. The State should continually review the threats and evaluate the implications of any changes to the threat assessment that may be needed. The State's competent authorities should take steps to ensure that any change is appropriately reflected in their regulatory framework and in the shipper's or carrier's physical protection measures. Recognizing that a revision of the DBT 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 DBT should then be reviewed in light of the revised threat assessment (para. 3.39 of Ref. [2]).

3.48. In the event of a change in the threat, especially one indicating a particular threat to nuclear material in transport, a State's competent authorities should consider directing a shipper or carrier to postpone or cancel a shipment.

Risk informed² approach for design of the physical protection system

3.49. The State should use a risk management approach to ensure that its physical protection regime is keeping the risk from the possibility of unauthorized removal or sabotage during transport at an acceptable level. This involves evaluating the threat and potential consequences of such acts and ensuring that appropriate physical protection measures are put in place to prevent or minimize the likelihood of a successful malicious act of these types (para. 3.41 of Ref. [2]).

² In this publication, the term 'risk informed' is used for consistency with the Nuclear Security Fundamentals [4]. The term 'risk based' is used in Ref. [2] for the same concept.

3.50. Risk management takes into account an assessment of risk, which may be quantitative or qualitative. Quantitative risk assessment involves determining the probability of an event occurring and multiplying it by the potential consequences of the event. The probability of a malicious act occurring or being attempted is very difficult to quantify, and therefore, in some cases, it is assumed to be one. Qualitative risk management involves consideration of the threat and potential consequences in order to identify high risk combinations (e.g. highly credible threat and severe consequences) on which efforts should be focused to minimize risk. Conversely, low risk combinations may be identified for which the graded approach should be applied and physical protection measures may not need to be as stringent (para. 3.41 of Ref. [2]).

3.51. The risk assessment identifies areas where additional measures should be taken to reduce the risk. Risk may be reduced through, for example, deterrence (e.g. by making apparent the robust physical protection measures in place), information security (e.g. by minimizing the information available about the nature and routing of the shipment), strengthening physical protection measures (e.g. by adding defence in depth, increasing the resistance of the conveyance and/or package to attack) and reducing potential consequences (e.g. by controlling the chemical or physical form of the material being transported) (para. 3.42 of Ref. [2]).

Fundamental Principle H: 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” [2].

3.52. The development of the State’s physical protection regime should be structured around a graded approach to provide higher levels of protection against events that could result in more severe consequences. In doing this, the State should consider what level of risk is acceptable and what level of protection against the threat should be provided (para. 3.43 of Ref. [2]).

3.53. For protection against unauthorized removal for use in a nuclear explosive device, the category of the nuclear material, as defined in Table 1 (see Section 4), reflects the relative difficulty of producing consequences from construction of a nuclear explosive device. Therefore, in accordance with the graded approach,

Category I nuclear material should be protected with the most stringent levels of physical protection, whereas materials less than Category III may only need to be protected with prudent management practices as defined in Ref. [9].

3.54. For protection against sabotage and unauthorized removal for subsequent dispersal, the State needs to consider the potential radiological consequences of such acts and define graded protection measures on this basis. The State should consider how to protect nuclear material, taking into account its potential to cause unacceptable radiological consequences, and ensure that protection measures are required for material capable of producing such consequences. Nuclear material with the potential to give rise to unacceptable radiological consequences should be protected with physical protection measures that are commensurate with those consequences. Reference [9], on security in the transport of radioactive material, provides guidance on this (para. 3.44 of Ref. [2]).

3.55. States should also consider using the concept of a graded approach to define the levels of administrative security measures such as information security (see paras 3.63–3.67) and determining the trustworthiness of individuals.

Fundamental Principle I: 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” [2].

3.56. The State should incorporate the concept of defence in depth in the preventive and protective measures that it requires for protection of nuclear material in transport. Defence in depth requires a designed combination of security equipment, procedures and administrative measures (including the organization of guards and the performance of their duties) and features of the transport equipment (including the conveyance, any protective overpacks and packages) that support security. The defence in depth approach should be incorporated in the design of the physical protection system to provide the functions of detection, delay and response. Each function should be provided by multiple independent measures so that failure of one measure does not lead to loss of that function. For example, detection may rely on observation by personnel and also use electronic measures to detect intrusion into the cargo compartment, and delay may be achieved through multiple independent physical barriers, such as the conveyance enclosure, protective overpacks and the package.

SUSTAINING THE PHYSICAL PROTECTION REGIME

Fundamental Principle F: 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” [2].

3.57. Nuclear security culture plays an important role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to prevent sabotage or the unauthorized removal of nuclear material and to detect and respond to any nuclear security events. A nuclear security regime includes a range of elements and activities, including:

- Legislation and regulation;
- Intelligence gathering;
- Assessment of the threat to nuclear material and nuclear facilities;
- Administrative systems;
- Various technical security systems;
- Response capabilities;
- Mitigation activities.

An effective nuclear security culture is dependent on education, training and awareness of people who plan, operate and maintain physical protection systems. Even a well designed system can be degraded if the procedures necessary to operate and maintain it are poor, or if the shipper or carrier fails to follow procedures. Ultimately, the physical protection regime depends on the people involved and their leaders, and this human factor should be addressed in efforts to enhance nuclear security culture.

3.58. As transport occurs in the public domain, it is important that everybody involved in transport operations is aware of the need to establish and maintain a strong security culture. Some States may choose to license carriers of nuclear material rather than rely on a shipper’s contractual conditions, and in such cases the competent authorities should consider how to address and promote a security culture among personnel who may have no nuclear background. This could be achieved by regular briefings on the current threats, to raise awareness of those involved, as well as imposing licence conditions designed to enhance the overall company security policy.

3.59. In transport operations, a strong safety culture is also important. A strong safety culture includes elements of openness and transparency with regard to information. Thus, a balance needs to be maintained towards the need for confidentiality of sensitive information, which is an important element of security culture. Safety and security culture should be built and maintained in an integrated manner to facilitate the management of safety–security interfaces.

Fundamental Principle J: 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” [2].

3.60. The State should, within its regulatory framework, require that a shipper or carrier establish and implement a quality assurance policy and programme to ensure that where a physical protection system is designed, implemented, operated or maintained, it is done so to a standard capable of effectively responding to the threat(s) identified by the threat assessment or DBT and that meets the State’s regulations.

3.61. A quality assurance programme should apply to all physical protection related activities (technical, procedural and administrative) and be reviewed on a periodic basis. For the transport of Category I nuclear material, shippers or carriers should ensure that all relevant physical protection measures (such as the tracking system and communications equipment) are operating correctly, and this should then be confirmed to the State’s competent authorities before transport commences.

3.62. Quality assurance programmes for safety are influenced by concepts of openness and transparency. While the quality assurance programmes for physical protection will be based on similar concepts, the need to protect the confidentiality of sensitive information will need to be taken into account. Quality assurance as well as safety and security culture should be integrated into an organization’s management system to ensure the management of safety–security interfaces.

Fundamental Principle L: 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” [2].

3.63. Each State should establish requirements for protecting the confidentiality of sensitive information relating to the transport of nuclear material. This may include information on:

- The DBT;
- General capabilities of the response forces;
- The TSP;
- The detailed nature, characteristics and quantities of nuclear material to be protected;
- The design and operation of the physical protection system for transport (e.g. drawings, diagrams or sketches that represent design features, or guard procedures);
- Specific information on particular shipments (i.e. timing, route schedules and itineraries, and contingency plans).

Using a graded approach, sensitive information relating to transport operations, including detailed information on the schedule and route, should only be disseminated to individuals who need to know this information (para. 3.53 of Ref. [2]).

3.64. The State should take steps, consistent with national requirements and procedures, to ensure appropriate protection of information relating to transport operations, the unauthorized disclosure of which could compromise the physical protection of nuclear material. This includes identifying what information needs to be protected and the level at which it should be protected, using a graded approach (see paras 3.52–3.55). In international transport operations, the State needs to take steps to ensure that the information will be protected at the same level by all of the States involved.

3.65. The State should define in its regulatory framework the provisions that a shipper or carrier should follow for ensuring the confidentiality of information relating to physical protection systems. Management of physical protection systems should limit access to sensitive information to those who need to know to perform their duties. It is particularly important that information addressing

possible vulnerabilities in physical protection systems should be protected, since it could assist an adversary in planning or performing a malicious act (paras 3.53 and 3.54 of Ref. [2]).

3.66. Occasionally, particularly for the transport of less than Category III or Category III nuclear material, information may need to be passed to various recipients for operational purposes (such as ferry bookings and transport network requirements), since these types of material are typically transported by commercial carriers under non-exclusive use conditions. Protection of this information should be proportionate to the risk associated with such material.

3.67. Sanctions against persons compromising the confidentiality of sensitive information should be part of the State's legislative or regulatory system, and should be severe enough to act as a deterrent against such actions. States should make such offences punishable by appropriate penalties, which take into account their potentially grave nature (para. 3.55 of Ref. [2]).

Sustainability programme

3.68. Sustaining the effectiveness of the State's physical protection regime is necessary to ensure that it remains effective in the long term. The State should establish a sustainability programme to ensure that the necessary resources are committed to this effort, including by shippers and carriers (para. 3.56 of Ref. [2]).

3.69. Shippers and carriers should have sustainability programmes for their physical protection systems that include:

- (a) Operating procedures and instructions to personnel (specific to role);
- (b) Human resources management and training;
- (c) Maintenance, updating, repair and calibration of equipment;
- (d) Performance testing and monitoring of operating systems;
- (e) Configuration management, to ensure that the physical protection systems (including computer systems) are configured as designed and that any changes are properly designed, verified and implemented;
- (f) Resource allocation to ensure continued effectiveness of the physical protection system (para. 3.57 of Ref. [2]).

PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

Fundamental Principle K: Contingency Plans

“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” [2].

3.70. The State should ensure that local authorities, the shipper, carrier and all others involved in the shipment are trained and prepared to respond if a malicious act occurs against a shipment of nuclear material. This should be achieved by contingency planning, which should include periodically testing and exercising contingency plans prior to undertaking shipments.

3.71. Contingency plans should be developed jointly by the State and local authorities and the shippers and carriers. They should be coordinated with the emergency plans for response to a nuclear or radiological emergency in line with the all hazards approach [8, 11]. Thus, the State’s regulatory framework should clearly specify the requirements for contingency planning: which contingency response capabilities are to be provided by the State and local authorities, which are to be provided by the private sector and how they are to be coordinated.

3.72. The goal of contingency planning is to ensure a timely and effective response at all levels in the event of a nuclear security event involving the transport of nuclear material. It is essential that the correct actions and decisions are taken at the right time to adequately respond to and resolve the situation. Arrangements should be made to ensure the continued effectiveness of the physical protection system during any emergency, through careful and integrated planning by the State, shipper and carrier (para. 3.61 of Ref. [2]).

Responsibilities of the State

3.73. The State should establish a contingency plan to respond to nuclear security events during the transport of nuclear material. This should consist of actions that are to be taken in the event of unauthorized removal or sabotage involving nuclear material in transport but are considered beyond the control or capabilities of the shipper or carrier. These plans should cover transport of nuclear materials both domestically and internationally. In addition, contingency plans should be harmonized with the national response plan for nuclear security events [5].

Responsibilities of the shipper or carrier

3.74. In accordance with the State's regulatory framework, a shipper or carrier should establish, implement and exercise contingency plans for the transport of nuclear material. These plans should cover the response to a range of scenarios and be approved by the State's competent authorities.

3.75. A clear chain of command should be established to respond to a nuclear security event during transport, with appropriate lines of communication.

3.76. Coordination between guards that may accompany shipments and response forces should be regularly exercised. Transport personnel should be trained and prepared to act in full coordination with the guards, response forces and other response teams in accordance with the contingency plan (para. 3.60 of Ref. [2]).

3.77. Whenever a malicious act is detected, the shipper or carrier should immediately initiate its contingency plan (para. 3.62 of Ref. [2]).

4. CHARACTERIZATION OF NUCLEAR MATERIAL FOR THE APPLICATION OF SECURITY IN TRANSPORT

4.1. Nuclear material should be characterized to determine appropriate physical protection requirements to prevent the unauthorized removal of material during transport based on:

- (a) Its potential for use in the construction of a nuclear explosive device;
- (b) The potential radiological consequences if it were subsequently dispersed or used for other malicious purposes.

4.2. In addition, the potential radiological consequences of sabotage of a shipment of nuclear material should be taken into account, and additional protective measures applied in those cases where the need for protection against sabotage warrants them (para. 6.3 of Ref. [2]).

4.3. This approach accounts for three primary ways in which nuclear material might be used in a malicious act. These three types of act are addressed in more detail in the following sections. Based on consideration of the nuclear security measures needed to protect nuclear material against these three types

of potential malicious act, the most stringent physical protection measures should be identified and applied.

NUCLEAR MATERIAL CATEGORIZATION AND AGGREGATION

Nuclear material categorization

4.4. The primary factor in determining the necessary physical protection measures against the unauthorized removal of nuclear material is the potential for the material to be used in a nuclear explosive device. Table 1 categorizes nuclear material on the basis of the element, isotope, quantity of material and irradiation (if any). This categorization provides a basis for specifying appropriate physical protection measures against unauthorized removal. However, there are other aspects of nuclear material that render it more, or less, attractive to an adversary, including physical and chemical form, and degree of dilution (paras 4.5 and 6.4 of Ref. [2]). By adjusting or subdividing the categories in Table 1, or by explicitly assigning particular materials to categories, the State may effectively define specific physical protection measures for each category of material.

4.5. Footnote f of Table 1 provides the option of lowering the nuclear material category for irradiated fuel by one category, but States should carefully consider whether or not to do this. The provision is based on the premise that radiation levels due to irradiated fuel are sufficient to incapacitate any adversary before a malicious act can be completed, but there are plausible scenarios in which an adversary with basic knowledge and resources could complete a malicious act before incapacitation due to radiation dose (para. 4.6 of Ref. [2]).

Nuclear material aggregation

4.6. During transport, different materials (plutonium, ^{235}U with different enrichments and ^{233}U) may be present in the same conveyance. The total amount of nuclear material in a single conveyance should be used in determining the categorization of the conveyance and, hence, in identifying appropriate physical protection measures for the conveyance. There are several mathematical approaches for calculating the aggregated category for the nuclear material, and a State should decide which approach it will use (para. 6.5 of Ref. [2]). In any approach, nuclear material that is in a form that is no longer usable for any nuclear activity, minimizes the potential for dispersal and is practicably irrecoverable should be protected in accordance with prudent management practice and need not be aggregated (para. 4.7 of Ref. [2]).

TABLE 1. CATEGORIZATION OF NUCLEAR MATERIAL

| Material | Form | Category I | Category II | Category III ^a |
|---------------------------|---|-------------------|---|------------------------------------|
| 1. Plutonium ^b | Unirradiated ^e | 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 | Unirradiated ^e | | | |
| | — Uranium enriched to 20% ²³⁵ U or more | 5 kg or more | Less than 5 kg but more than 1 kg | 1 kg or less but more than 15 g |
| | — Uranium enriched to 10% ²³⁵ U but less than 20% ²³⁵ U | n.a. ^d | 10 kg or more | Less than 10 kg but more than 1 kg |
| | — Uranium enriched above natural but less than 10% ²³⁵ U | n.a. ^d | n.a. ^d | 10 kg or more |
| 3. Uranium-233 | Unirradiated ^e | 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 | | | Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content) ^{e, f} | |

(The categorization of irradiated fuel in this 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)

Source: Table 1 of Ref. [2].

^a Quantities not falling in Category III, natural uranium, depleted uranium or thorium should be protected at least in accordance with prudent management practice.

^b All plutonium except that with isotopic concentration exceeding 80% in ²³⁸Pu.

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

^d n.a.: not applicable.

^e 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.

^f 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 1 m unshielded.

4.7. One approach to aggregation is a set of formulas that are derived from Table 1. In this approach, an aggregation of different materials in the same consignment should be classified as outlined:

(a) Category I if:

$$\frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%) }{5000} \geq 1 \quad (1)$$

(b) Category II if:

$$\begin{aligned} & \frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%) }{1000} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{10\,000} \geq 1 \\ & > \frac{\text{Pu} + {}^{233}\text{U}}{2000} + \frac{{}^{235}\text{U}(\geq 20\%) }{5000} \end{aligned} \quad (2)$$

(c) Category III if:

$$\begin{aligned} & \frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%) }{15} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{1000} + \\ & + \frac{{}^{235}\text{U}(> U_{\text{nat}} \text{ and } < 10\%) }{10\,000} \geq 1 \\ & > \frac{\text{Pu} + {}^{233}\text{U}}{500} + \frac{{}^{235}\text{U}(\geq 20\%) }{1000} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{10\,000} \end{aligned} \quad (3)$$

(d) Less than Category III if:

$$\begin{aligned} 1 > & \frac{\text{Pu} + {}^{233}\text{U}}{15} + \frac{{}^{235}\text{U}(\geq 20\%) }{15} + \frac{{}^{235}\text{U}(\geq 10\% \text{ and } < 20\%) }{1000} + \\ & + \frac{{}^{235}\text{U}(> U_{\text{nat}} \text{ and } < 10\%) }{10\,000} \end{aligned} \quad (4)$$

or if the material consists only of natural uranium, depleted uranium or thorium,

where

| | |
|---|---|
| Pu | is the mass in grams of all plutonium except that with isotopic composition exceeding 80% in ^{238}Pu ; |
| ^{233}U | is the mass in grams of ^{233}U ; |
| $^{235}\text{U} (\geq 20\%)$ | is the mass in grams of ^{235}U present in a form enriched to 20% ^{235}U or more; |
| $^{235}\text{U} (\geq 10\% \text{ and } < 20\%)$ | is the mass in grams of ^{235}U present in a form enriched to 10% ^{235}U or more, but less than 20% ^{235}U ; |
| $^{235}\text{U} (> U_{\text{nat}} \text{ and } < 10\%)$ | is the mass in grams of ^{235}U present in a form enriched above natural but less than 10% ^{235}U ; |

and the denominators are masses in grams.

4.8. Note that the above formulas are not precise in all cases when a quantity of nuclear material is exactly the same as the denominator in the equation. Table 1 should be consulted when the quantity is exactly the same as the threshold mass that defines the category for a given material and the numerical result of applying the equation is very close to 1. Some denominators in the formulas need to be interpreted as ‘greater than’ or ‘less than’ values, whereas others need to be ‘greater than or equal to’ or ‘less than or equal to’.

Examples

4.9. In example 1, the material has a mass of 5 kg and consists of 4 kg of uranium enriched to greater than 20% and 1 kg of plutonium (see Eq. (5)). Using the Category I equation (see Eq. (1)):

$$\frac{1000 (\text{Pu})}{2000} + \frac{4000(^{235}\text{U}(\geq 20\%))}{5000} \geq 1 \quad (5)$$

so the mixture is Category I.

4.10. In example 2, the material has a mass of 3 kg and consists of 2.5 kg of uranium enriched to greater than 20% and 500 g of plutonium (see Eq. (6)). Using the Category II equation (see Eq. (2)):

$$\begin{aligned} \frac{500 (\text{Pu})}{500} + \frac{2500(^{235}\text{U}(\geq 20\%))}{1000} &\geq 1 \\ &> \frac{500 (\text{Pu})}{2000} + \frac{2500(^{235}\text{U}(\geq 20\%))}{5000} \end{aligned} \quad (6)$$

so the mixture is Category II.

4.11. Another approach for determining the category of aggregated nuclear material uses the following formula:

$$\frac{1}{S} = \sum_i \frac{f_i}{S_i} \quad (7)$$

where

f_i (dimensionless) is the mass fraction of material type i of the mixture (mass of each material type present divided by the total mass of material present);

S_i (kg or g) is the mass threshold for material type i for the category being considered, as listed in Table 1;

and S (kg or g) is the mass threshold for the aggregation of material for the category being considered, as listed in Table 1.

4.12. To determine the applicable nuclear material category using this approach, the methodology should be first to check whether the aggregated nuclear material is Category I and then, if necessary, continue with Category II, Category III and less than Category III.

4.13. Step 1: A material, or a mixture of materials, is Category I if the aggregated mass on board a conveyance is greater than or equal to the Category I mass threshold calculated by the above formula for the material or mixture (see Eq. (7)). If it is not Category I, proceed to step 2.

4.14. Step 2: A material, or a mixture of materials, is Category II if the aggregated mass on board a conveyance is greater than or equal to the Category II mass threshold calculated by the above formula for the material or mixture (see Eq. (7)). If it is not Category II, proceed to step 3.

4.15. Step 3: A material, or a mixture of materials, is Category III if the aggregated mass on board a conveyance is greater than or equal to the Category III mass threshold calculated by the above formula for the material or mixture (see Eq. (7)). If the mass of the material or mixture of materials is below the Category III mass threshold, it is less than Category III.

Examples

4.16. Using example 1, the material has a mass of 5 kg and consists of 4 kg of uranium enriched to greater than 20% and 1 kg of plutonium. The mass fraction of uranium enriched to greater than 20% is 4/5 and for plutonium is 1/5.

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{4/5}{S_{U-235}} + \frac{1/5}{S_{Pu}} = \frac{4/5}{5 \text{ kg}} + \frac{1/5}{2 \text{ kg}} = 0.26$$

Therefore, $S = 3.85$ kg. Since the mass of the material (5 kg) is greater than S (3.85 kg), it is above the threshold for Category I for this mixture, and the shipment is Category I.

4.17. Using example 2, the material has a mass of 3 kg and consists of 2.5 kg of uranium enriched to greater than 20% and 500 g of plutonium. The mass fraction of uranium enriched to greater than 20% is 2.5/3 (or 5/6) and for plutonium is 0.5/3 (or 1/6).

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{U-235}} + \frac{1/6}{S_{Pu}} = \frac{5/6}{5 \text{ kg}} + \frac{1/6}{2 \text{ kg}} = 0.25$$

Therefore, $S = 4$ kg. The total mass is 3 kg, which is below the mass threshold for the mixture for Category I.

Step 2: The Category II mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{U-235}} + \frac{1/6}{S_{Pu}} = \frac{5/6}{1 \text{ kg}} + \frac{1/6}{0.5 \text{ kg}}$$

Therefore, $S = 0.86$ kg. The total mass is 3 kg, which is above the mass threshold for the mixture for Category II. Therefore, the mixture is Category II.

POTENTIAL ADDITIONAL PHYSICAL PROTECTION MEASURES FOR CATEGORY III AND LESS THAN CATEGORY III NUCLEAR MATERIAL

4.18. The widespread dispersal of some nuclear materials (e.g. plutonium) in Category III (≤ 500 g) or less than Category III (≤ 15 g) could have sufficiently severe consequences that the level of protection that should be given to prevent its acquisition for use in a nuclear explosive device is less stringent than the level of protection that should be given to prevent its use in a malicious act involving dispersal (unauthorized removal for use in a radiological dispersal device, or sabotage). When considering the level of protection for such material, consideration should be given to the quantity of material that if stolen or dispersed in an act of sabotage could cause unacceptable radiological consequences.

4.19. For example, 499 g of plutonium (the limit of Category III nuclear material) will have an activity about 15 000 times the A_2 value and consequently is recommended to be protected at the “enhanced security level” for radioactive material [9, 12]. The A_2 values for individual radionuclides are found in table 2 of the IAEA Transport Regulations [10]. The enhanced security level entails physical protection measures beyond those needed for Category III nuclear material, such as the preparation and use of a transport security plan (TSP).

4.20. Similarly, for some nuclear materials in quantities below Category III (≤ 15 g ^{233}U or Pu), protection based on the nuclear material categorization will not be sufficient to account for their potential radiological consequences. These materials should be protected at least to the “basic security level” (see section 4.2 of Ref. [9]) and may warrant the “enhanced security level” (see section 4.3 of Ref. [9]), depending on the activity of the shipment and the State’s threat assessment.

4.21. One process for determining which physical protection measures should be applied is:

- (a) Determine the nuclear material category, taking into account all of the nuclear material on board the conveyance during shipment and using the aggregation formulas if needed:

- (i) In the case of Category I and II nuclear material, the necessary physical protection measures are determined based on the nuclear material category.
 - (ii) In the case of Category III or less than Category III nuclear material, the security level and the corresponding physical protection measures are identified as described in (b).
- (b) Determine the security level for the shipment based on its radiological properties: This can be done by determining the number of A_2 values on board the conveyance. Divide the total activity (TBq) of each radionuclide on the conveyance by the A_2 value (TBq) for that radionuclide. The result is the number of A_2 values on the conveyance for that radionuclide. Sum the number of A_2 values for all radionuclides to determine the total number of A_2 values on board the conveyance as follows:

$$\text{Total no. } A_2 \text{ values} = \sum_i \frac{A(i)}{A_2(i)} \quad (8)$$

where $A(i)$ is the total activity (TBq) for each radionuclide on the conveyance, and $A_2(i)$ is the A_2 value (TBq) for that radionuclide.

Alternatively, an effective A_2 value for the collection of radionuclides on board can be calculated and, when divided into the total activity of all radionuclides on the conveyance, will give the total number of A_2 values present (see para. 405 of the IAEA Transport Regulations [10]):

- (i) If the number of A_2 values is greater than or equal to 3000, the enhanced security level should be applied to account for the radiological properties of the shipment.
- (ii) If the number of A_2 values is less than 3000, the basic security level should be applied, or if the material, based on its radioactive properties, need only be subjected to prudent management practices (in accordance with Ref. [9]), these measures should be applied.
- (iii) Determine the physical protection measures needed based on the nuclear material category and the radioactive material security level.

4.22. A State may determine that consideration of other factors is necessary, which may lead to further categorizations based on these other factors. Each categorization is used to define the physical protection measures appropriate for the risk being protected against. The most stringent of the applicable measures should be applied to a given shipment.

POTENTIAL RADIOLOGICAL CONSEQUENCES OF SABOTAGE

4.23. In addition to the physical protection measures that should be applied on the basis of the nuclear material categorization or the potential radiological consequences (see paras 4.18–4.22), some shipments may present significant potential radiological consequences in the case of an act of sabotage (para. 6.3 of Ref. [2]).

4.24. The State should identify which shipments it considers warrant protection against sabotage due to the potential to cause unacceptable radiological consequences. States may reach different conclusions on what constitutes unacceptable radiological consequences. Consideration should be given to factors such as:

- (a) Package contents (i.e. radionuclides, physical and chemical forms);
- (b) Package and conveyance design;
- (c) Effect of the postulated sabotage event(s) on the contents–package–conveyance combination;
- (d) Location where the act of sabotage may occur (e.g. in a highly populated area if transport of such material is allowed in these areas);
- (e) Postulated threat;
- (f) State’s definition of unacceptable radiological or other consequences.

4.25. Section 8 provides additional guidance on how potential radiological consequences from acts of sabotage can be determined and appropriate physical protection measures that the State might require.

IDENTIFICATION OF APPLICABLE PHYSICAL PROTECTION MEASURES

4.26. The measures to protect against unauthorized removal (see paras 4.18–4.22 and Section 6) and sabotage (see paras 4.23–4.25 and Section 8) should be compared and the more stringent measures implemented in an integrated manner (see para. 6.57 of Ref. [2]). In some cases, there may be need for additional measures against sabotage, such as additional protection against stand-off attacks. In other cases, the measures for protection against sabotage may be of the same nature but more stringent; for example, more thorough surveillance of the route in advance of the shipment.

4.27. The State should ensure that the appropriate physical protection measures are applied to each shipment of nuclear material, taking into account all of the properties of the nuclear material being transported. Figure 1 illustrates the sequence of considerations in determining the physical protection measures applicable to a shipment, taking into account all of the potential risks.

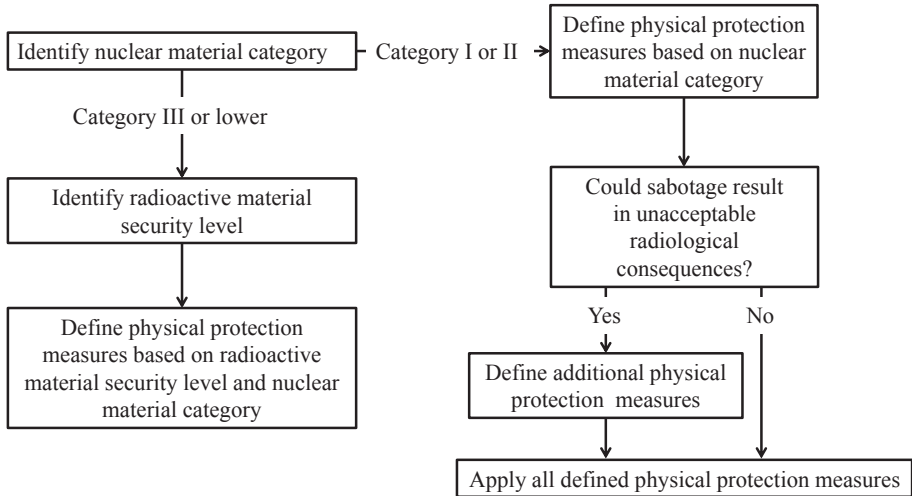


FIG. 1. Defining physical protection measures to account for all risks.

5. DEVELOPMENT AND IMPLEMENTATION OF ELEMENTS OF A PHYSICAL PROTECTION REGIME FOR THE TRANSPORT OF NUCLEAR MATERIAL

5.1. This section explains the provisions that the competent authorities may require from shippers, carriers and receivers (and others as required by the State), to establish and maintain a sound nuclear security culture and an effective physical protection system for the transport of nuclear material. Paragraphs 5.3–5.13 address different approaches to specifying and applying physical protection measures. Paragraphs 5.14–5.23 address responsibilities, including specific responsibilities of shippers, carriers and receivers for the physical protection in the transport of nuclear material. Paragraphs 5.24–5.30 discuss the key functions and objectives that may be specified by the competent authorities for a physical protection system. Paragraphs 5.31–5.39 address the development of a transport

security plan (TSP), including the process of submitting a TSP to the competent authorities for obtaining approval and the implementation of a TSP.

5.2. The physical protection measures for shippers, carriers and receivers recommended in this Implementing Guide should be in addition to measures established for safety purposes. Physical protection measures should not replace safety measures resulting from States' requirements or the IAEA Transport Regulations [10], except where approved by the transport safety competent authority; for example, the use of compensatory measures for the removal of placards on high risk shipments (para. 3.17 of Ref. [2]).

SPECIFYING AND APPLYING PHYSICAL PROTECTION

5.3. A State should base its physical protection regime on a current evaluation of the threat. Consequently, a State should ensure that it bases its transport security requirements on an evaluation of the threat. There are three distinct approaches for specifying requirements to address the threat: the prescriptive approach, the performance based approach and the combined approach.

The prescriptive approach

5.4. The prescriptive approach is for the State to establish specific physical protection measures to meet its defined objectives for each category of nuclear material. The prescriptive approach places the prime responsibility for nuclear security directly on the State (or its competent authorities), which decide(s) what measures should be in place to manage the risk. The State provides a set of 'basic' provisions for the shipper or carrier to apply for the transport of each category. A set of recommended basic provisions is provided in Section 6.

5.5. Advantages of the prescriptive approach include simplicity in implementation for both the competent authorities and the shipper or carrier, elimination of the need to transmit sensitive information in the form of results of a threat assessment or design basis threat (DBT), and ease of inspection and auditing. The main disadvantage of the prescriptive approach is its relative lack of flexibility in addressing specific circumstances. The major expenditure of time and effort in the prescriptive approach is by the competent authorities to define the required nuclear security measures.

5.6. The prescriptive approach may be particularly appropriate in cases where the combination of threat and potential consequences is low — for example, where shipments of Category III nuclear material take place in a relatively stable sociopolitical environment — or where conducting a detailed threat assessment or establishing a State DBT is not practicable.

The performance based approach

5.7. In the performance based approach, the competent authorities define the physical protection objectives to be met on the basis of a national threat assessment and, where applicable, a DBT. The shipper or carrier is responsible for defining nuclear security measures for the transport of nuclear material that meet these objectives to the satisfaction of the competent authorities.

5.8. The performance based approach allows flexibility for the shipper or carrier to propose a particular combination of physical protection measures. The adequacy of these measures is then evaluated against the threat assessment or DBT. This will ensure that performance based measures meet the set objectives and provide an analysis of the physical protection system designed to satisfy the five key functions of deterrence, detection, assessment, delay and response to a malicious act.

5.9. The advantages of the performance based approach are that it allows flexibility for an effective physical protection system to be composed of a combination of physical protection measures appropriate to each shipper's or carrier's particular circumstances. The performance based approach is also the most cost effective approach for a knowledgeable shipper or carrier.

5.10. Disadvantages of the performance based approach are that it depends upon both the shipper or carrier and the competent authorities having relatively high levels of security expertise, and that the competent authorities must divulge some sensitive information from the State's threat assessment or DBT to the shipper or carrier, who, therefore, needs the capabilities to provide adequate protection of this sensitive information. Furthermore, the competent authorities need more time to assess and approve each proposal submitted by a shipper or carrier.

The combined approach

5.11. The combined approach includes elements from both the prescriptive and performance based approaches. There are many variants of the combined approach, of which three examples are provided:

- (a) The competent authorities may require application of a performance based approach for the transport of nuclear material having the most severe potential consequences of malicious acts, while applying a prescriptive approach where the potential consequences are less severe.
- (b) The competent authorities may require that a basic set of prescriptive requirements be supplemented by using the performance based approach to address particular matters such as the current threat.
- (c) The competent authorities may provide physical protection objectives and a set of physical protection measures for each required security function. The shipper or carrier may then choose the particular measures to apply, but must demonstrate that the resulting physical protection system, as a whole, meets the objectives.

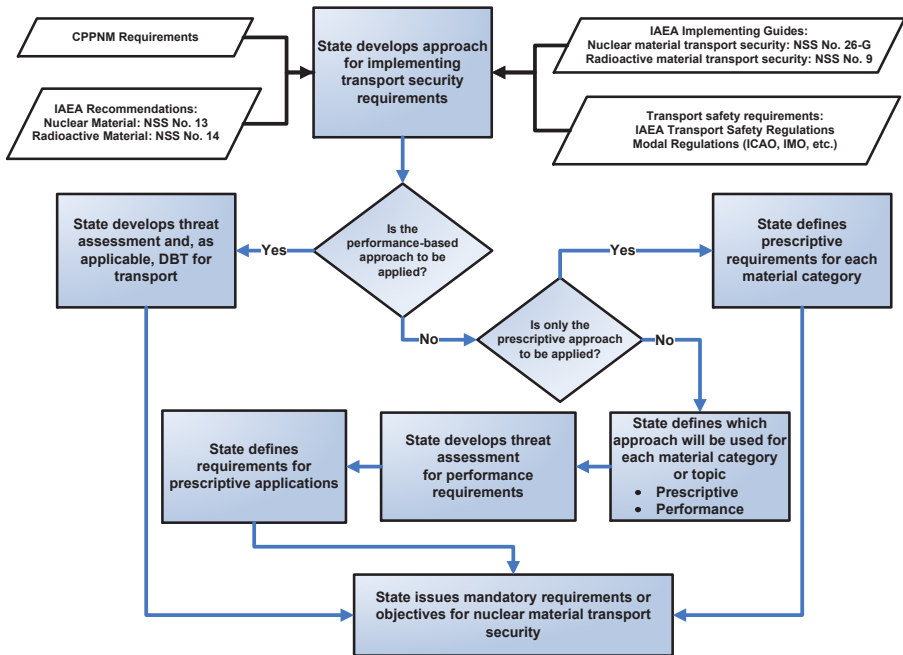
5.12. The main advantage of the combined approach is the flexibility that it allows. It potentially imposes a lesser burden on both the State's competent authorities and the shippers or carriers, since aspects of the prescriptive and performance based approach can be applied to those cases for which each approach is more suitable. Basic nuclear security measures to address lower risks and constant threats can be addressed through the prescriptive approach, and the performance based approach can be used to supplement or modify these measures as necessary for higher risks and changing threats.

Process for applying the approaches

5.13. The process that a State may follow in deciding which approach to use is shown in Fig. 2. The figure highlights the decisions that need to be made by the competent authorities regarding which approach to use and, if the combined approach is chosen, the decisions on which approach is to be used for each category of nuclear material.

RESPONSIBILITIES FOR PHYSICAL PROTECTION IN TRANSPORT

5.14. Physical protection responsibilities for the planning and implementation of the transport of nuclear material should be clearly assigned by the State or its competent authorities. The details of which responsibility is assigned to whom will vary from State to State. General responsibilities that the State may assign include those for developing a TSP, providing advance notification of shipment details to the receiver and completing other relevant technical, procedural and administrative actions. In addition to these general responsibilities, there are specific responsibilities that should be assigned to the shipper, carrier or receiver.



Note: CPPNM — Convention on the Physical Protection of Nuclear Material; ICAO — International Civil Aviation Organization; IMO — International Maritime Organization.

FIG. 2. Decision process for determining the regulatory approach to transport security.

5.15. The entity responsible for the physical protection of a shipment (normally the shipper or carrier) should develop a TSP in accordance with the State’s regulatory framework. States should require a TSP for the transport of Category I and II nuclear material. Information on how to develop a TSP can be found in paras 5.31–5.39.

5.16. In accordance with the State’s regulatory framework, the entity responsible for nuclear security of a shipment should give the receiver advance notification of the shipment details and the expected time of arrival, and should subsequently inform the receiver of any changes to that information.

Specific responsibilities of the shipper

5.17. Prior to transporting nuclear material, the shipper should ensure that all the necessary permits and authorizations have been obtained. If also responsible for physical protection, the shipper should ensure that all measures and arrangements

for the security of the shipment are in place. If handing over to a carrier who is responsible for physical protection, the shipper should ensure that the carrier concerned is authorized to transport nuclear material.

Specific responsibilities of the shipper or carrier

5.18. Prior to commencing transport, the shipper or carrier should verify that all physical protection measures are in accordance with the TSP or the State's physical protection requirements. If the physical protection measures do not provide the required level of protection, the shipper or carrier should immediately correct the situation, inform the competent authorities and, if necessary, postpone the shipment (paras 3.30 and 6.23 of Ref. [2]).

5.19. During the transport of nuclear material, the shipper or carrier is responsible for continuously monitoring the conveyance. This will enable the shipper or carrier to react to any unauthorized interference with, or attempt to access, the nuclear material or the conveyance transporting nuclear material.

5.20. The shipper or carrier should conduct inspections of the conveyance prior to commencing transport, after any stops (scheduled and unscheduled) and on arrival at its destination. This will allow the shipper or carrier to determine any loss of or damage to, or tampering with, packages during transport or on delivery. Further information on inspections and searches can be found in paras 6.39–6.44.

5.21. The shipper or carrier should inform the receiver or other responsible organization, specified in the TSP, of any unforeseen changes to the expected time of arrival.

Specific responsibilities of the receiver

5.22. The receiver should be prepared to secure the shipment on arrival and have appropriate personnel available to receive the nuclear material at the prearranged place, date and time.

5.23. The receiver should report to the shipper and/or carrier that all packages have been received intact. If packages are found to be missing or to have been tampered with, the receiver should immediately contact the appropriate response organizations and the competent authorities.

KEY FUNCTIONS OF A PHYSICAL PROTECTION SYSTEM

5.24. Shipments of nuclear material need defence in depth against unauthorized removal, sabotage and other intentional malicious acts. The key functions of physical protection are deterrence, detection, assessment, delay and response. These functions apply to all categories of nuclear material, but they should be implemented in a graded manner, taking account of the State's threat assessment.

Deterrence

5.25. Physical protection measures for transport should include features that are visible and are intended to deter malicious acts as well as providing protection if such acts are attempted. These features could include visible physical protection measures built into the conveyance, and the use of guards and convoys. Such measures may also perform other physical protection functions, but they should not affect the safety design of the transport packages.

Detection

5.26. Activities directed towards the detection of unauthorized removal, sabotage and other intentional malicious acts should start before the nuclear material is placed in the conveyance. Using a graded approach, conveyances, equipment and personnel involved in a shipment should undergo a thorough inspection before departure. This will ensure that the conveyance remains uncompromised prior to departure, thereby reducing the likelihood of malicious acts.

5.27. Using a graded approach, the shipper or carrier of the conveyance and/or the guards involved in the shipment should provide continuous surveillance of the conveyance and the surrounding area. This can be achieved through the use of technical measures such as detection or tracking devices and communications systems, and human observation.

Assessment

5.28. Assessment is the examination of information received from detection alarms and/or observations, and is undertaken to determine whether a security response is required. Information received from detection alarms, observations and other sources should be assessed rapidly to ensure a timely response.

Delay

5.29. Physical protection measures in transport should delay an adversary attempting to commit a malicious act sufficiently to enable an appropriate and effective response to the attempt. The length of delay needed will depend on the time needed for response forces to respond, and this should reflect a graded approach, taking into account the category of the nuclear material and the postulated threat capabilities.

Response

5.30. The response to a nuclear security event during the transport of nuclear material may come from accompanying guards and/or response forces. Response activities should aim to prevent the completion of a malicious act, or to mitigate its consequences, and to locate and recover any missing material.

DEVELOPING THE TRANSPORT SECURITY PLAN

5.31. The TSP should document all physical protection measures and arrangements necessary to adequately address the security requirements and/or objectives of the State. The TSP should identify responsibilities for all aspects of the protection of nuclear material in transport. The State determines who is responsible for preparing and maintaining the TSP. This will normally be the shipper or carrier having direct responsibility for the security of the nuclear material in any particular mode or phase of the transport.

5.32. An assessment of potential vulnerabilities prior to a shipment takes into account all information, as appropriate, regarding the mode(s) of transport, the route to be followed, any transit sites, overnight stops, temporary storage or transfer areas, and planned or potential stopping places (e.g. for refuelling or rest). Other parts of the transport system that affect its vulnerability include the conveyances, equipment and personnel involved in the shipment, the capabilities of the transport control centre, the response forces and the operating conditions during transport. The result of this assessment is then used to assess the effectiveness of the shipper's or carrier's physical protection system in one or more scenarios that represent credible nuclear security events derived from the threat assessment or DBT, and to make a judgement as to whether the overall effectiveness of the physical protection system is adequate or whether improvements such as compensatory measures are needed.

5.33. The TSP should include procedures for reporting non-compliances by the shipper or carrier during transport to the competent authorities [5].

5.34. The TSP should be protected as sensitive information and should only be discussed with other organizations in so far as it applies to their roles and responsibilities. The TSP may, for example, be divided into several parts and only the relevant parts shared with particular organizations. For information security reasons, the State may require that the TSP be developed in the form of a series of separate documents.

Submitting and obtaining approval of the transport security plan

5.35. The State will specify whether a TSP and any associated vulnerability assessment are to be submitted to the competent authorities for review and approval. This may depend on the category of nuclear material being proposed for transport. Such a review could be an iterative process. If the competent authorities consider that the State requirements are not met by the TSP or that the results of the vulnerability assessment are inadequate, the TSP and/or vulnerability assessment should be returned to the originator for modification.

5.36. For the transport of all Category I and, as appropriate, Category II nuclear material, a TSP should be submitted by the shipper or carrier to the competent authorities for approval or endorsement in accordance with the State's requirements. A TSP may cover a single shipment or a series of similar shipments.

5.37. The process of developing and, when required, obtaining approval of a TSP is shown in Fig. 3.

Implementing the transport security plan

5.38. Once the TSP (and, if required, the vulnerability assessment) have been submitted and, if required, approved by the competent authorities, detailed plans and preparations for the shipment can proceed. Physical protection measures for the shipment should be undertaken in accordance with the TSP and associated written instructions and agreements. If for any reason the shipment cannot be completed in accordance with the TSP, the shipper or carrier should immediately implement compensatory measures to maintain the level of protection and, if necessary, postpone the shipment and inform the competent authorities. The competent authorities may require the shipper or carrier to prepare a set of compensatory measures in advance (para. 3.30 of Ref. [2]).

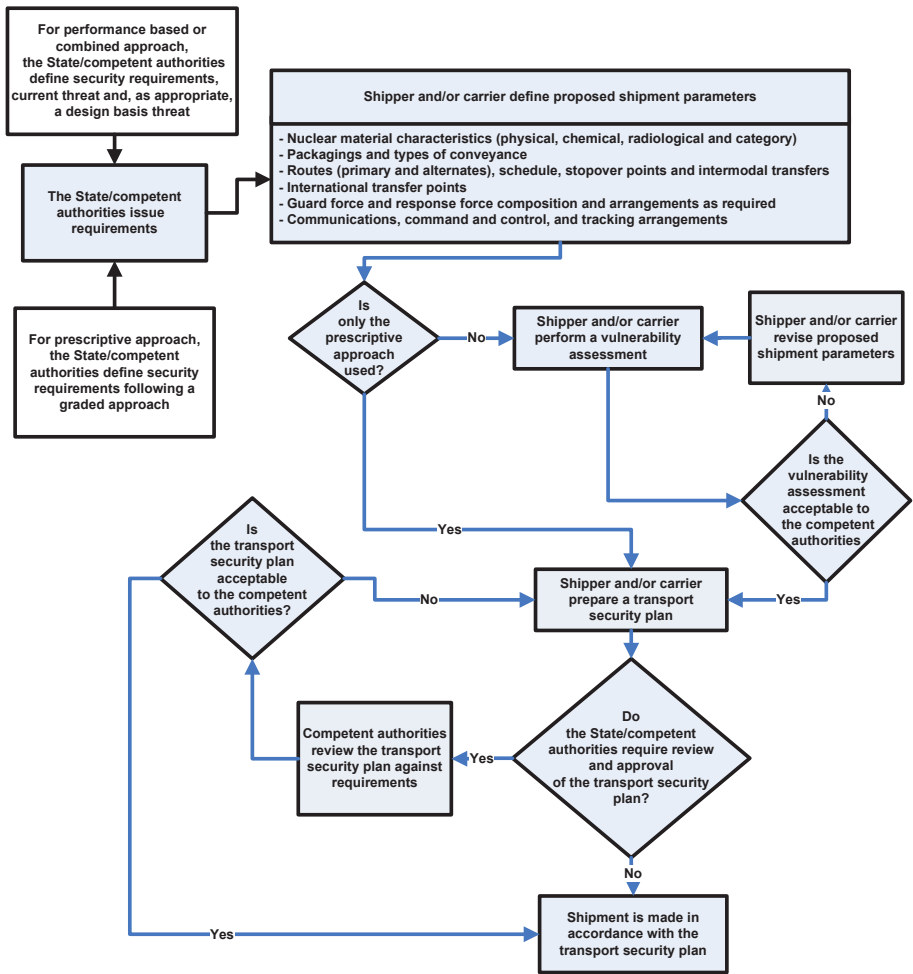


FIG. 3. Sample process for competent authorities' review and approval of a vulnerability assessment, if needed, and a transport security plan.

5.39. If any incidents or unscheduled delays occur during transport, a review of physical protection arrangements should be conducted in order to evaluate the effectiveness of the TSP and to identify any necessary improvements that may be made to improve its effectiveness for future shipments.

6. MEASURES AGAINST THE UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN TRANSPORT

6.1. The specific physical protection measures to be taken will depend on the category of nuclear material being shipped. Common basic measures should be applied to all shipments of nuclear material, and additional specific measures of increasing stringency should be applied successively for Category III, II and I nuclear material. This section suggests a set of provisions that a State should consider when defining physical protection requirements for all categories of nuclear material in transport.

6.2. The measures described in this section should be treated as baseline measures applicable in all cases of the transport of nuclear material. The State may wish to add further provisions for particular categories of nuclear material or to define the State's physical protection requirements in more detail than is done in Ref. [2]. In each case, the State should take account of the attractiveness of the nuclear material to an adversary, the potential threat to the shipment, local circumstances and the results of the State's threat assessment and/or design basis threat (DBT). Other physical protection measures than those described in this section may be required by the State, particularly if protection against sabotage is determined to be necessary (see Section 8).

6.3. There is a close interrelationship between many of the provisions in this section. For example, for shipments of Category I nuclear material, the conveyance, guards, communications capabilities, transport control centre and the response forces should be integrated into a physical protection system that can prevent adversaries from removing the nuclear material or hijacking the conveyance. The more numerous, better armed and better trained the accompanying guard force is, the less the likelihood that the guards could be overcome. However, where there are constraints on the size or arming of the guard force, then increased dependency should be placed on ensuring that the conveyance is designed to resist or delay attack from a determined adversary until arrival of the response forces.

6.4. The provisions in this section are specified by topic to allow emphasis to be placed on the graded approach for establishing a physical protection system to protect against the unauthorized removal of nuclear material. Physical protection measures against sabotage are described in Section 8.

6.5. Paragraphs 6.6–6.70 present suggested provisions that are dependent on the category of nuclear material to be transported but independent of the mode of transport, paras 6.71–6.108 provide suggested provisions that are mode dependent, and paras 6.109–6.112 present additional physical protection measures based on potential radiological consequences from unauthorized removal and subsequent dispersal. Within each of these subsections, the nuclear security functions are discussed in turn, defining suggested provisions for Category III nuclear material, and then more stringent suggested provisions for higher categories. The competent authorities may, as appropriate, modify or eliminate specific provisions for a given category of nuclear material.

MODE INDEPENDENT PROVISIONS

6.6. The State is responsible for ensuring that prudent management practices are applied during transport for all nuclear material, including:

- (a) Quantities of nuclear material less than in Category III;
- (b) Natural uranium, depleted uranium and thorium;
- (c) Nuclear material which is in a form that is no longer usable for any nuclear activity minimizes the potential for dispersal and is practicably irrecoverable (footnote a of Table 1 and para. 4.7 of Ref. [2]).

6.7. Prudent management practices include those normal commercial practices implemented by shippers and carriers to protect the material being shipped as an asset. These include accepting responsibility for the safe keeping of the material while it is under their control and protecting it against loss or theft in a manner commensurate with its monetary value. The material should also be shipped in accordance with applicable dangerous goods regulations [10, 13, 14], particularly those applicable to radioactive material; inter alia, requirements for classification, packaging, shipping documents, marking and labelling will apply. These requirements inform carrier personnel of the need to handle and transport the packages with due care and diligence, providing a graded level of protection against unauthorized removal.

Common requirements

6.8. There are several recommended common requirements for the transport of nuclear material (see paras 6.6–6.10 of Ref. [2]) that should be considered when planning and making shipments. When applying these recommendations, the State should apply the graded approach and consider what is “operationally

practicable” [2], particularly for shipment of material that is less than Category III or in Category III. These types of material are typically transported by commercial carriers under non-exclusive use conditions and the practicalities of commercial shipping should be considered in light of the relatively low risks posed by the lower category materials. For Category II and I nuclear material, the common requirements should be applied more rigorously.

6.9. Physical protection measures against unauthorized removal during all transport of nuclear material should include, as far as operationally practicable and in accordance with the graded approach (para. 6.6 of Ref. [2]):

- (a) Minimizing the total time during which the nuclear material remains in transport. This helps to minimize the time during which the material is outside a protected facility and the time during which an adversary might attempt to obtain it while in transport.
- (b) Minimizing the number and duration of transfers (such as transfer from one conveyance to another, transfer to and from temporary storage, and temporary storage while awaiting the arrival of the conveyance).
- (c) Protecting nuclear material during transport and in temporary storage in a manner consistent with the category of that nuclear material.
- (d) Avoiding predictable movement schedules by varying times and routes. Transport by rail, sea and air may be dependent on regularly scheduled conveyances, but predictable shipment patterns should be avoided if possible.
- (e) Requiring prior determination of the trustworthiness of individuals involved in the transport of nuclear material. Considering the wide range of persons involved in transport activities, including international transport, States should apply a graded and flexible approach in the determination of its trustworthiness policy, commensurate with State laws and regulations (para. 3.14 of Ref. [2]).
- (f) Limiting advance knowledge of information about the transport to the minimum number of individuals necessary.
- (g) Using a transport system with passive and/or active physical protection measures appropriate for the threat assessment or DBT. For shipments of smaller quantities of nuclear material, consideration may be given to the protection afforded by the conveyances normally used by the carriers (e.g. vehicles with locked cargo compartments).
- (h) Using routes that 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. A State may determine that certain categories of nuclear material require continuous surveillance. Shipments of smaller quantities of nuclear material using non-exclusive use conveyances may not need to be continuously attended (e.g. when the driver is making a delivery), but the time during which they are unattended should be minimized.

6.10. When a series of shipments is planned by a shipper, it should be ensured when deciding the number and nature of the shipments that security is not compromised for operational convenience. For example, operational considerations might suggest that a shipper make a series of Category III nuclear material shipments rather than a single Category II nuclear material shipment. However, in deciding whether this is acceptable from a security perspective, consideration should be given to the prevailing threat, the resources available to deal with potentially simultaneous nuclear security events and the amount of material in transit at any given time.

Selection of transport mode and routing

Provisions for Category I and II nuclear material

6.11. In determining the mode(s) of transport and routing to be used in the transport of nuclear material, the shipper should identify and evaluate the characteristics of the proposed shipment that could affect the ability to protect the shipment against the potential threats involved. The mode(s) and route(s) of the transport should be identified and the conditions under which an alternative route(s) would be used should be determined (para. 6.22 of Ref. [2]). In choosing the route and mode, consideration should be given to:

- (a) The security situation along the entire route; for example, avoiding areas where there are known threats or areas where security cannot be ensured;
- (b) Response force capabilities and the time needed for response forces to reach any point along the route;
- (c) The practicality of the route, including acceptance by any transit States and their ability and willingness to ensure security during transit.

Assessment and approval of the transport security plan

Provisions for Category I and II nuclear material

6.12. The State should require that a TSP be developed and submitted for approval. The TSP may be developed and submitted by the shipper and/or the carrier, depending on who the competent authorities assign these responsibilities to. The competent authorities should define the content of the TSP, the process for submitting it and how any revisions required by the competent authorities should be incorporated. Threat assessment is an important input to the TSP development and review process (para. 6.22 of Ref. [2]).

6.13. While the TSP may refer to other national plans, such as those for police or other response actions, the competent authorities may wish to verify that all necessary coordination and/or agreements with other involved agencies are in place.

6.14. The required content of the TSP should be specified in detail. Topics that may need to be described in detail in the TSP include:

- (a) Training and exercises;
- (b) Pre-operational testing of physical protection equipment;
- (c) Trustworthiness and verification of the identity of personnel;
- (d) Physical protection measures to be applied;
- (e) Contingency plans, including their coordination with emergency plans;
- (f) Trans-shipment terminals;
- (g) Intermodal transfers.

For international shipments, references should be made to any intergovernmental agreements governing responsibilities and transfer of responsibilities. Additional details on the content of the TSP are provided in Appendix I.

6.15. Through their review of the TSP, the competent authorities may identify parts of the plan that they consider warrant exercises to evaluate the adequacy of the security arrangements (in addition to any exercises already included in the TSP). The competent authorities should ensure that such exercises are completed, the results documented and any necessary improvements identified, and any necessary changes incorporated into the TSP. Similarly, the competent authorities may require that vulnerability assessments be performed on any parts of the plan that they consider warrant more detailed analysis, such as those relating to stopping points, route selection and intermodal transfer points.

6.16. Information in the TSP will be sensitive, particularly information on the route and schedule of shipments. This information should be identified, marked and handled in accordance with the State's requirements for protecting the confidentiality of sensitive information.

Additional provisions for Category I nuclear material

6.17. Approval by the competent authorities of the TSP should be based on a detailed examination of the proposed physical protection measures to ensure that they are adequate to prevent unauthorized removal. These measures should provide sufficient delay so that guards and/or response forces have time to intervene before unauthorized removal could be completed. The TSP should include details of the mode and route of transport, including any alternative route(s), arrangements for using alternative routes and the conditions under which they would be used, stopover facilities and intermodal transfers. The TSP should include arrangements for making changes to the itinerary, such as alteration of the route during shipment, in response to unexpected changes in the physical environment, threat assessment or operating conditions (para. 6.33 of Ref. [2]).

6.18. The competent authorities should ensure that any intergovernmental agreements, particularly those applicable to armed guards and transfer of responsibilities for armed response, are reflected in the TSP.

Authorization of shipments

Provisions for Category I nuclear material

6.19. Authorization by the competent authorities for a shipment should be required prior to commencing transport. The competent authorities' decisions should be based on the current threat assessment and intelligence information and, where appropriate, on a detailed surveillance of the route to observe the current environment. The authorization for a shipment may include specific limitations and conditions related to the particular circumstances (para. 6.34 of Ref. [2]).

6.20. The competent authorities should specify the process for obtaining authorization of a shipment and what information is to be submitted to support an application for such authorization. In its evaluation of such an application, the competent authorities should review the latest threat information and conditions along the route to ensure that the nuclear security measures specified in the TSP will provide adequate security during the transport.

Advance notification and coordination

Provisions for Category I, II and III nuclear material

6.21. The shipper or carrier should give the receiver advance notification of the planned shipment, specifying the mode of transport at arrival (road, rail, water or 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 (para. 6.12 of Ref. [2]). The shipper or carrier should also provide advance notification to the competent authorities.

6.22. Physical protection measures for nuclear material in transport should include a prior agreement between the shipper, receiver and carrier on the time, place and procedures for transferring nuclear security responsibilities (para. 6.13 of Ref. [2]). Such an agreement may be based on normal commercial practices and responsibilities.

6.23. Shippers or carriers should only transfer nuclear material packages to other carriers that are known to them to be bona fide carriers. In the case of transport using a carrier based in a different State from the shipper, the suitability of the carrier should be confirmed with the competent authorities of the shipper's State, who may base such confirmation on consideration of that carrier's experience with similar transports or information exchange with the competent authorities of the carrier's State.

Additional provisions for Category I and II nuclear material

6.24. The receiver should confirm readiness to accept the delivery (and handover, if applicable) at the expected time, prior to the commencement of the shipment. In some cases, formal agreements may be required, and if so, these should be strictly followed. It is particularly important that transport schedules be maintained where such agreements are involved (para. 6.21 of Ref. [2]).

Locks, seals, alarms and engineered systems

Provisions for Category I, II and III nuclear material

6.25. In compliance with transport safety requirements, the outside of every package containing nuclear material "shall incorporate a feature such as a seal that

is not readily breakable and which, while intact, will be evidence that the package has not been opened” (para. 637 of the IAEA Transport Regulations [10]). However, most seals do not provide an immediate indication of intrusion. They can only indicate that intrusion may have occurred, and only when they are physically checked. Seals should therefore not be viewed as a substitute for intrusion detection and/or surveillance.

6.26. 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. Whenever it is necessary to use open conveyances, the load should be covered or hidden from view unless this would compromise the safety of the transport package (para. 6.14 of Ref. [2]).

6.27. Where practicable, locks and seals commensurate with the categorization of the nuclear material being transported 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. When enclosed freight containers are used, verification of the integrity of a door seal should be sufficient in lieu of verifying each individual seal on packages inside the freight container on which that door seal is fitted (para. 6.15 of Ref. [2]).

6.28. 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 (para. 6.9 of Ref. [2]).

6.29. 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 (para. 6.18 of Ref. [2]).

6.30. The security level of locks should follow the graded approach, based on the category of the nuclear material in the package. Lock fittings and components, such as attachment points and tie-down attachments, should be complementary to the quality and strength of the required locks.

6.31. Engineered systems that are designed or intended to fulfil physical protection functions should be appropriate to all of the proposed modes of transport. In addition, the shipper or carrier should ensure that any devices, equipment or arrangements employed to deter, detect, delay and respond to theft of the conveyance or its nuclear cargo, including any locks and seals on packages, freight containers, compartments or conveyances transporting Category III nuclear material, are operational and effective prior to dispatch and where feasible during transport.

Additional provisions for Category I and II nuclear material

6.32. The physical protection measures applied to the transport system (conveyance, freight container and/or package) should include delay measures to increase the time required by an adversary to complete the unauthorized removal of the nuclear material. The delay should be sufficient to allow guards and/or response forces the time needed to make an appropriate response (para. 6.25 of Ref. [2]).

6.33. The competent authorities should consider requiring the use of electronic intrusion detection and duress alarms.

6.34. High strength and high security locks should be required on packages for Category I and II nuclear material.

Additional provisions for Category I nuclear material

6.35. Engineered alarm or intrusion detection systems should be applied to conveyances to the extent practicable. These systems should be redundant, and capable of being monitored from the transport control centre.

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 two different keys to be unlocked held by two different authorized persons (the ‘two-person rule’). The locking devices should not interfere with the safety performance of the package (para. 6.36 of Ref. [2]).

Written instructions

Provisions for Category I, II and III nuclear material

6.37. The shipper or carrier should provide consignment specific transport documents to appropriate carrier personnel. These documents should include any information, for example regarding required actions in the event of an accident or nuclear security event, that has not already been covered in prior training or general instructions. Drivers or operators of all conveyances used should be given emergency contact information for the areas through which they will be passing. The information may be part of other instructions or manuals, such as shipboard emergency procedures. The documents should be provided in the languages deemed necessary by the shipper, carrier or the authorities concerned and any confidentiality requirements should be followed.

Additional provisions for Category I and II nuclear material

6.38. Written instructions detailing physical protection responsibilities (consistent with the TSP) should be appropriately classified and provided in advance of the shipment to all personnel with such responsibilities, including staff of the transport control centre or alternative central point of communication, carriers, guards and response force personnel. If the competent authorities require prior approval of those instructions, they should be reviewed and approved by the competent authorities. In such cases, the content of the instructions and the procedure for approval should be specified by the competent authorities (para. 6.27 of Ref. [2]).

Inspections, searches and surveillance

Provisions for Category I, II and III nuclear material

6.39. 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. Personnel of the shipper or carrier should undertake periodic inspections and security searches at appropriate times — including after loading but before dispatch and during transport — verifying that all specified physical protection measures on the conveyances are effective and that there has been no tampering with the load or conveyances. In many cases, it will be sufficient for the shipper

or carrier to perform a visual inspection based on their own knowledge of the conveyance. If during an inspection any physical protection measure is found to be ineffective, a decision should be made to provide compensatory measures that maintain the required level of physical protection of the shipment or, if the failure is sufficiently serious, that the shipment be stopped until the failed measure is operating effectively (para. 6.16 of Ref. [2]).

Additional provisions for Category I and II nuclear material

6.40. The conveyance should be searched immediately prior to loading and dispatch. Appropriately trained personnel may be needed to ensure that the conveyance has not been tampered with in any way. Immediately following completion of the search, the conveyance should be placed in a secure area or kept under guard surveillance until loading (para. 6.26 of Ref. [2]).

6.41. Prior to commencing transport, the carrier should verify that all physical protection measures are in place in accordance with the TSP. Inspections should be made before dispatch of each nuclear material consignment to confirm the integrity of the locks and seals on the package, freight container, compartment and conveyance. These inspections should be undertaken in accordance with the information and procedures provided in the TSP (para. 6.23 of Ref. [2]).

6.42. Physical protection measures should include continuous and effective surveillance of the cargo, load compartment and/or conveyance. States are encouraged to use guards for such surveillance. Surveillance may include use of remote technologies such as closed circuit television and detection technologies such as video motion detection. The guards should respond to any anomalies reported as part of the surveillance activity (para. 6.20 of Ref. [2]).

Additional provisions for Category I nuclear material

6.43. Security inspections should be performed on all equipment, stores, personal effects and other goods loaded onto the conveyance.

6.44. Guards providing surveillance should do so under conditions which ensure close communication with response forces.

Communication and confidentiality involving the shipper, carriers and receiver

Provisions for Category I, II and III nuclear material

6.45. Consideration should be given to using a method for periodically identifying the location (e.g. using bar code tracking systems) of a shipment of nuclear material. Information concerning the location of the shipment should be properly controlled but should be readily available to the shipper and/or carrier, and should be provided to the receiver when appropriate.

Additional provisions for Category I and II nuclear material

6.46. Consideration should be given to using a method for providing continuous tracking of the location (e.g. satellite based tracking systems) of a shipment of nuclear material.

6.47. Consideration should be given to establishing a transport control centre or other central point of communication to monitor and coordinate voice and/or digital communications between personnel involved with a specific shipment or group of shipments, to monitor positional tracking, and to facilitate command and control. The role of the transport control centre in the case of a nuclear security event involving the nuclear material in transport should be clarified to ensure effective coordination with the emergency response.

6.48. Physical protection measures should include the provision of continual, two way voice communication between the conveyance, any guards accompanying the shipment, the designated response forces and, where appropriate, the shipper and/or receiver (para. 6.29 of Ref. [2]).

Additional provisions for Category I nuclear material

6.49. There should be a transport control centre for the purpose of tracking the current position and security status of the shipment of nuclear material, alerting response forces in the case of an attack and maintaining continual, secure, two way voice communication with the shipment and the response forces.

6.50. The transport control centre should be protected so that its function can continue in the presence of the threat. It should be physically protected from attack, provide access control for staff and other authorized personnel, and be alarmed with a monitored security system. While the shipment is in progress,

the transport control centre should be staffed by qualified personnel and any other personnel designated by the competent authorities whose trustworthiness has been determined (para. 6.37 of Ref. [2]).

6.51. The transport control centre should use redundant communications channels and be equipped with a source of emergency electrical power. Multiple communications systems using different equipment, frequencies and technologies can mitigate the effects of any interference, jamming, lost signals and gaps in coverage. No communications channel can ensure complete information security, but the use of encryption technologies, coding or secure channels can counteract monitoring and make real time interception and monitoring extremely difficult.

6.52. The capabilities of the transport control centre should be matched to the size and complexity of the transport operations, the anticipated threats, the communications needs of the response organizations, and the existing communications infrastructure of the State(s) involved. Continual two way communication systems between the conveyance, transport control centre, guards accompanying the shipment, designated response forces and, where appropriate, the shipper and/or receiver should be redundant, diverse and secure (para. 6.38 of Ref. [2]).

6.53. An individual should be specifically designated in the TSP with the responsibility to report frequently to the transport control centre and on the arrival of the shipment, at each stopover and at any handover of responsibility for the shipment. This communication should be performed in accordance with the TSP (para. 6.39 of Ref. [2]).

Guards

Provisions for Category I, II and III nuclear material

6.54. 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. The graded approach, based on the category of nuclear material, should be used in specifying the physical protection measures necessary to accomplish this. For example, for lower category nuclear material, it may not be necessary for guards to accompany the shipment if the competent authorities determine that response forces are sufficient (para. 6.17 of Ref. [2]).

6.55. The use of guards to accompany shipments of Category III nuclear material may be considered. If guards do not accompany the shipment, the driver or operator of the conveyance, or another designated crew member, should be capable of providing surveillance of the nuclear material and making all required notifications in the case of a nuclear security event.

Additional provisions for Category II nuclear material

6.56. 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. If guards are not armed, compensatory measures should be applied, such as additional monitoring and delay features (para. 6.24 of Ref. [2]).

Additional provisions for Category I nuclear material

6.57. Appropriately equipped and trained guards 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 guards at all times, especially when the conveyance is not in motion. The guards should respond to any anomalies reported as part of the surveillance activities. States are encouraged to use armed guards to the extent that laws and regulations permit. When guards are not armed, compensatory measures should be applied, such as adding delay barriers to the conveyance exterior structure and/or interior cargo area and the use of non-lethal incapacitating agents. Guards' capabilities should be established with due consideration of the number of load carrying conveyances in the shipment (para. 6.35 of Ref. [2]).

6.58. 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 (para. 6.39 of Ref. [2]).

Response forces

Provisions for Category I, II and III nuclear material

6.59. The shipper and carrier should maintain and have readily available, to the extent possible, accurate information on how to summon local response forces close to the route being used.

Additional provisions for Category I and II nuclear material

6.60. Arrangements should be made to provide adequately sized, equipped and trained response forces to deal with nuclear security events. Such events could occur anywhere along a transport route, which may extend over a significant distance and include remote areas, thereby giving an adversary a wide choice of potential attack locations. At some locations, it may be particularly difficult for adequate response forces to arrive within a useful period of time, in which case alternative response forces would need to follow the transport convoy at a reasonable distance. The objective should be the arrival of the response forces in time to prevent the unauthorized removal of nuclear material (para. 6.30 of Ref. [2]). In accordance with the graded approach, the competent authorities may allow differences in the size and capabilities of response forces for Category I and II nuclear material. Based on the State's assessment of the threat, if the guards have sufficient capability to counter the threat, designated response forces may not be necessary. The required level of assurance that unauthorized removal will be prevented may also be different for Category I and II nuclear material.

Measures after transport

Provisions for Category I, II and III nuclear material

6.61. The receiver should inspect the integrity of the shipment upon its arrival and notify the shipper of the arrival. This inspection should include verifying the receipt of all expected packages and contents.

6.62. If the shipment does not arrive at its intended destination within the interval of time agreed in advance by the shipper, receiver and, as appropriate, the competent authorities, the receiver should notify the shipper, the carrier and the competent authorities.

6.63. Any deficiencies in the physical protection system noted during transport should be corrected or appropriate compensatory measures taken before any subsequent transport is undertaken and should be reported to the competent authorities.

Additional provisions for Category I nuclear material

6.64. The person designated in the TSP should report to the transport control centre, by an appropriate communications channel in accordance with the information provided in the TSP, the arrival of the shipment at its destination and the completion of the handover of the shipment.

6.65. A review of the TSP and overall conduct of the shipment should be conducted and communicated to the competent authorities after transport is completed. The shipper or carrier should take into account the feedback of experience from completed shipments to identify and implement improvements in planning for future shipments of a similar nature.

Unplanned stops

6.66. If the conveyance makes an unexpected extended stop, the physical protection measures appropriate for that category of nuclear material in storage should be applied to the extent practicable. The 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 for nuclear material in use and storage (para. 6.10 of Ref. [2]).

Information security and computer security

6.67. 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. Appropriate security measures should be applied to sensitive information related to the transport of nuclear material. Such information includes the physical protection measures in place, including the capabilities of the response forces and of measures for detection, assessment and delay. Information security measures should ensure protection of the confidentiality, integrity and availability of the sensitive information. Sensitive information should be identified and appropriate protective measures defined

using a graded approach related to the potential impact of the compromise of the information (para. 6.7 of Ref. [2]).

6.68. Computer systems are used in many aspects of transport operations, including the processing and storing of sensitive information, the tracking of shipments, the management of access controls to such shipments and the monitoring of materials. Measures should be taken to ensure the security of all electronic systems, particularly computer systems. Measures should be in place that provide assurance for both information security and for computer security. Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, provides details on the implementation of such measures [15].

6.69. It should be ensured as far as possible that shipments are conducted in a manner that includes elements of unpredictability to make it difficult for an adversary to plan an attack effectively. Information on routes and schedules is therefore particularly sensitive and should be protected accordingly. 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. In many cases, the external markings (i.e. placards) on conveyances are to alert emergency responders to the presence of radioactive material. Alternative measures may be used to accomplish this function, such as emergency response personnel accompanying the shipment, or communications arrangements that would allow transmission of this information in the case of an accident. If alternative measures acceptable to the transport safety competent authority are in place, external markings may not be necessary (para. 6.7 of Ref. [2]).

6.70. 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 (para. 6.7 of Ref. [2]).

MODE SPECIFIC PROVISIONS

6.71. In addition to the mode independent provisions described above, the following provisions should be considered depending on the mode or modes of transport to be used in the shipment.

Additional provisions for road transport

Provisions for Category I, II and III nuclear material

6.72. If road movements cannot be completed without overnight or extended stops, or if there is a requirement to place nuclear material in temporary storage while en route (i.e. at a transfer point), then the nuclear material should be protected during such stops or storage in a manner that is consistent with storage measures that would be employed at a nuclear facility and to the extent practicable and consistent with the potential consequences of a malicious act against the material.

Additional provisions for Category I and II nuclear material

6.73. Transport of nuclear material by road should be on conveyances operated under exclusive use conditions (para. 6.31 of Ref. [2]).

6.74. During planned stops exceeding a certain duration to be defined in regulation, or storage en route of shipments of Category I and II nuclear material, a temporary protected area may be established (or an existing protected area, such as at a nuclear facility or military base may be used), to which access is restricted and which is under surveillance by guards that are in close communication with response forces. If the nuclear material is to remain on the load carrying vehicle, then the vehicle should be secured in order to deter or delay any unauthorized movement of the vehicle. Temporary storage arrangements for such stops should be approved in advance by the competent authorities as part of the TSP.

6.75. If an overnight stop is necessary, prior arrangements should be made for such a stop, which should be at an appropriately equipped and secured road stopover facility. During such stops, the load carrying road vehicle should be immobilized and guarded or parked in a secure, locked and guarded building or facility. Planned stopover locations and arrangements should be organized in advance.

Additional provisions for Category I nuclear material

6.76. Consignments of Category I nuclear material should preferably be transported on conveyances that are specifically designed to resist attack by equipping them with technical measures to deter, detect and delay access to the shipment, and that are equipped with a vehicle disabling device. A guard

or crew member, in addition to the driver, with formal security responsibilities should travel in each load carrying vehicle. The vehicle driver and accompanying person should be capable of activating the response to a nuclear security event according to the TSP (para. 6.40 of Ref. [2]).

6.77. Each load carrying vehicle should be accompanied by a minimum of one separate vehicle containing guards. Effective, protected communication between all vehicles in the convoy should be provided. Accompanying guards should conduct surveillance of the route for any indicators of a threat, protect the load carrying vehicle and be prepared to initiate an appropriate response. Route surveillance may be performed from an unmarked vehicle travelling some distance in front of the load carrying vehicle and escort vehicle, or from aircraft (para. 6.40 of Ref. [2]).

6.78. Consideration should also be given to:

- (a) Limiting the number of load carrying vehicles in any one convoy;
- (b) Using a lead reconnaissance vehicle that travels in advance of the convoy to assess the current situation along the route, raise alarms as needed, redirect the convoy if necessary and initiate response force actions as required;
- (c) Having a minimum of two people travel in each vehicle in the convoy, so each person would be capable of detecting and responding to an unauthorized action by the other.

6.79. To prevent tampering and protect information on the design of the physical protection equipment, the conveyance should be protected from unauthorized access or observation even when it is not occupied.

6.80. During the planning process, 'safe havens' should be identified along the route that can be used if necessary during emergencies or other unplanned stops.

6.81. For shipments of Category I nuclear material, the transport vehicle should be equipped with security features approved by the competent authorities that permit immobilization of the cab or the load carrying part of the vehicle. This provision should apply to all vehicles used in such a shipment. Immobilization means rendering the loaded transport vehicle incapable of movement under its own power. The purpose of this is to deny an adversary who may succeed in gaining control of a transport vehicle the ability to move the vehicle.

6.82. The immobilization mechanism should be operated only when it is apparent that an attempt is being made to gain unauthorized control over the shipment. Immobilization should not be initiated in a way that would endanger the driver, escorts or members of the public. Immobilization procedures should be developed and incorporated into the TSP. Operation of the immobilization mechanism and the procedures governing its use should be covered in the training for escorts and for drivers. The immobilization technique should meet the following criteria:

- (a) The immobilization device and procedure should be operated and performed from inside the cab of the vehicle by one person.
- (b) Immobilization should be accomplished within a short period of time (no more than several seconds) after the immobilization procedures are initiated.
- (c) After immobilization is accomplished, skilled technical personnel should not be able to return the transport vehicle to normal operating conditions in less time than it would take for the response forces to reach the vehicle. It should not be possible, by coercion of the drivers or escorts, for an adversary to bypass the effects of the immobilization or to significantly shorten the time needed to make the vehicle operational.
- (d) The device should pose no significant safety hazard before, during or after the immobilization.

6.83. Devices employed to immobilize vehicles may be mechanical or electrical. They should be relatively simple and reliable to operate so that they can be activated quickly under stressful conditions.

Additional provisions for rail transport

Provisions for Category I, II and III nuclear material

6.84. If rail movements cannot be completed without overnight or extended stops, or if nuclear material needs to be placed in temporary storage while en route (i.e. at a transfer point), then the nuclear material should be protected during such stops or storage in a manner that is consistent with storage measures that would be employed at a nuclear facility, to the extent practicable and consistent with the potential consequences of a malicious act against the material.

Additional provisions for Category I and II nuclear material

6.85. Packages containing Category I and II nuclear material should be carried in enclosed, locked rail vehicles or freight containers under exclusive use conditions, unless overriding safety considerations necessitate alternative measures providing an equivalent level of security (para. 6.31 of Ref. [2]).

6.86. If an extended stop is necessary, prior arrangements should be made for such a stop, which should be at an appropriately equipped and secured rail stopover facility. Such a stopover facility should be in a rail siding or terminal area, and security arrangements should be approved in advance by the competent authorities. During such stops, the load carrying rail vehicle should be guarded or positioned in a secure locked and guarded rail yard, building or facility (para. 6.6 of Ref. [2]).

Additional provisions for Category I nuclear material

6.87. Rail shipments should, as far as operationally practicable, be uninterrupted from origin to destination, with any planned stops being kept to a minimum and included in the TSP, which is approved by the competent authorities. During any stops, extra vigilance should be maintained.

6.88. Load carrying rail vehicles should be specifically designed to resist attack by equipping them with technical measures to detect, deter and delay access to the shipment. Guards accompanying the shipment should:

- (a) Travel on the train close to the conveyance to allow effective surveillance and response to an attack;
- (b) Be capable of communicating with the train engineer;
- (c) Be capable of initiating the appropriate response if an attack occurs.

6.89. To prevent tampering and information on the design of the physical protection equipment, the rail carriage should be protected from unauthorized access or observation even when it is not occupied.

Additional provisions for maritime transport

6.90. Although there are no additional International Maritime Organization regulations on security of nuclear material in transport, the following international instruments may be noted:

- Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation [16];
- International Convention for the Safety of Life at Sea (as amended) [17];
- International Ship and Port Facility Security Code [18];
- International Maritime Dangerous Goods Code [14].

6.91. Shippers should only consign nuclear material for international maritime transport to ships flagged to States that have made provisions for the physical protection of the nuclear material.

Additional provisions for Category I and II nuclear material

6.92. As far as operationally practicable, transport of nuclear material on inland waterways should be avoided.

6.93. Consideration should be given to: (i) having guards accompanying the shipment travel on the load carrying ship; and (ii) designing and equipping the container, compartment and/or ship to resist attack.

6.94. The nuclear material should be placed in a secure compartment or freight container which is locked and sealed. Packages of nuclear material should be situated within the ship, such that they are protected by the design of the ship, so as to delay any attack. If an extended stop is necessary, prior arrangements should be made for the stop, which should be at an appropriately equipped and secured maritime stopover facility. Security arrangements should be approved in advance by the competent authorities for any stopover facility. During such stops, the load carrying ship should be docked in a secure port facility (para. 6.6 of Ref. [2]).

6.95. The appropriate authorities should be alerted, as soon as possible, of any unscheduled stop of a maritime shipment of Category I or II nuclear material. If scheduled or unscheduled stops occur in a country other than the shipping country, the appropriate authorities in both the shipping country and the country where the stop occurs should be notified.

Additional provisions for Category I nuclear material

6.96. Maritime transport of Category I nuclear material should be conducted on a dedicated ship. During Category I shipments, the only other acceptable cargo should be other categories of nuclear material. The ship should be specifically

designed or modified to resist attack and to carry nuclear cargo (paras 6.31 and 6.42 of Ref. [2]).

6.97. Security personnel should search:

- (a) All personal items as they are brought on board the ship;
- (b) All persons entering the secure area;
- (c) All stores for the voyage as they are brought on board the ship.

6.98. Prior to commencing loading of the shipment, security personnel should also search:

- (a) Dockside areas adjacent to the ship;
- (b) Compartments adjacent to that containing the nuclear material;
- (c) The whole ship, including stores and the engine room;
- (d) The underwater section of the ship's hull.

6.99. Containers, compartments and/or ships used in the maritime transport of Category I nuclear material should be designed and equipped to resist attack by equipping them with technical measures to detect, deter and delay access to the shipment. The measures may include additional robust structures incorporated in the container or compartment design and systems for detecting and communicating abnormal events.

6.100. Critically sensitive areas and systems, such as the engine room, navigation bridge, communications areas and guards' positions, should be secured with limited access and should be kept locked at all times during transport. The ship should have a hardened control room for the purpose of command and control of the guards. The control room should be staffed by the guards' command staff and, where possible, be in a location near the centre line of the ship with other compartments around it to prevent disablement of the control room by attack from outside the ship, and delay any attack from within the ship.

6.101. Guards should accompany the maritime shipment on the load carrying ship and/or on an accompanying ship in a location where they can best respond to an attack, in accordance with the information provided in the TSP. Guards should be able to communicate with the captain and bridge as well as the transport control centre, and should be capable of activating any active detection and communication systems, the features of which should be clearly defined in the TSP.

6.102. Consideration should be given to providing the load carrying ship with the means that will allow the crew and the guards to be aware of any ship or aircraft that might be approaching, particularly on the high seas.

6.103. Ports of call along the route should be avoided.

6.104. To prevent tampering and protect information on the design of the physical protection equipment, the ship should be protected from unauthorized access or observation even when it is not occupied.

Additional provisions for air transport

Provisions for Category I, II and III nuclear material

6.105. For air transport of nuclear material, shipment should be conducted in accordance with the applicable security provisions in annex 17 of the Convention on International Civil Aviation [19, 20]. Loading should be arranged, as far operationally practicable, in such a way that the nuclear material does not need to be unloaded at stopovers.

6.106. If stops and/or changes of aircraft are necessary, consideration should be given to making prior arrangement for the physical protection of the consignment during ground operations and any necessary temporary storage, consistent with the category of the nuclear material (para. 6.6 of Ref. [2]).

Additional provisions for Category I and II nuclear material

6.107. Shipments should be made in aircraft designated for cargo only, in a secure compartment or container that is locked and sealed (para. 6.31 of Ref. [2]).

Additional provisions for Category I nuclear material

6.108. Shipments should be made in aircraft designated for cargo only and for which the nuclear material is its sole cargo. Air shipments of nuclear material should be made in an aircraft whose flag State is a State Party to the Convention on International Civil Aviation [19] (para. 6.43 of Ref. [2]).

ADDITIONAL PHYSICAL PROTECTION MEASURES BASED ON POTENTIAL RADIOLOGICAL CONSEQUENCES

6.109. Some nuclear material in Category III or less than Category III should be subject to additional physical protection requirements based on the potential radiological consequences if they were to be intentionally dispersed. The widespread dispersal of plutonium in Category III (≤ 500 g) or less than Category III (≤ 15 g) could result in sufficiently high radiological consequences that the level of protection appropriate to prevent its acquisition for use in a nuclear explosive device is less stringent than that appropriate to prevent its use in a radiological dispersal device. In these cases, the materials should be categorized based on their radiological properties, and the protection measures recommended in Ref. [9] should be applied in addition to the measures recommended in this publication. Paragraphs 4.18–4.22 provide guidance on the process that can be used to make this determination.

6.110. Based on its potential radiological consequences, some material below Category III may fall into the “basic security level” as defined in Ref. [9]. This would imply that in addition to prudent management practices, the following physical protection measures should be applied:

- (a) Basic security awareness training for all personnel involved;
- (b) Verification of the identity of all personnel involved;
- (c) Verification of security of conveyances used;
- (d) Written instructions;
- (e) Exchange of information on security measures between operators, shippers or carriers and with competent authorities ensuring the need for confidentiality;
- (f) Determining the trustworthiness of the personnel involved.

6.111. Similarly, some Category III material may have potential radiological consequences that place it in the “enhanced security level”, and more stringent physical protection measures than those described for Category III material in this publication are recommended in Ref. [12] and described in detail in Ref. [9]. These measures include:

- (a) Identification of shippers and carriers;
- (b) TSPs;
- (c) Advance notification of shipment;
- (d) Use of tracking devices;
- (e) Communications from the conveyance;

- (f) Additional security provisions for transport by road, rail and inland waterway to ensure that devices, equipment and other arrangements to deter, detect, delay and respond to malicious acts are effective at all times.

6.112. The physical protection measures recommended for the basic and enhanced security levels are described in Ref. [9].

7. MEASURES TO LOCATE AND RECOVER NUCLEAR MATERIAL MISSING OR STOLEN DURING TRANSPORT

STATES' RESPONSIBILITIES

7.1. The State's physical protection regime should include provisions for providing information and technical assistance to support rapid and comprehensive measures for locating and recovering missing or stolen nuclear material. The State should ensure within its regulatory framework that shippers, carriers and receivers are required to report lost, missing or stolen nuclear material. The roles and responsibilities for recovery of nuclear material should be clearly established (para. 3.9 of Ref. [2]).

7.2. Personnel with physical protection responsibilities should be given written instructions detailing their responsibilities in the event of missing or stolen nuclear material during transport.

7.3. When there is transboundary movement of nuclear material, there should be appropriate coordination between the States, and clear responsibilities for the location and recovery of nuclear material out of regulatory control [5]. States should cooperate with each other in locating and recovering lost or missing nuclear material. Once the location of the material has been identified in a particular State, that State becomes the lead in recovering and securing the material.

7.4. When it is reported to a State that nuclear material is missing or has been stolen, the State should notify the relevant international organizations and other States in accordance with international obligations and national legislation. The State should, considering international commitments and national legislation, inform bordering States of the event so that they may alert their law enforcement organizations, and draw upon their capabilities for monitoring for nuclear

material. Once a package has been reported to be lost, missing, misplaced or stolen during transport, the situation is out of the shipper's or carrier's control. The State should therefore implement the recommendations in Ref. [5].

7.5. A State that locates and recovers nuclear material that has been reported lost or stolen from another State should safely and securely store the material and, where appropriate, work with the State in which the control was lost to arrange the safe and secure return of the material. Actions taken by States holding the material should be consistent with national policies and procedures, and with applicable bilateral and multilateral agreements [5].

7.6. 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 nuclear material that goes missing or is stolen during transport. The State should clearly specify the requirements for location and recovery actions, as well as the response capabilities that will be provided by the State and those to be provided by the shipper or carrier, and how these are to be coordinated. In particular, the contingency plans should be harmonized with the national nuclear security response plan and the plans of the individual competent authorities responsible for implementing the national response plan for nuclear security. The State should also ensure that these contingency plans are coordinated with emergency response plans [7, 8].

7.7. The State should clearly define roles and responsibilities of appropriate State organizations for the location and recovery of missing or stolen nuclear material. Where different State organizations have different contingency plans, they should all be coordinated with the shipper's or carrier's contingency plans (para. 6.46 of Ref. [2]).

7.8. Contingency plans for locating and recovering lost nuclear material should be reviewed, and updated if necessary, on a regular basis (para. 6.51 of Ref. [2]).

7.9. The State should arrange regular exercises with the appropriate State entities to validate the contingency plans for locating and recovering nuclear materials and to train personnel in how to react in such a situation (para. 6.50 of Ref. [2]).

CARRIERS' RESPONSIBILITIES

7.10. 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 (para. 6.52 of Ref. [2]).

7.11. If a carrier suspects that a package containing nuclear material has been lost or removed from a conveyance, it is the carrier's responsibility to initiate an immediate search and to notify the competent authorities. Once it has been verified that a package is no longer under the carrier's control, the carrier should immediately notify the relevant authorities and the shipper. If all packages are found to be still under the carrier's control, the carrier should inform the relevant authorities and the shipper (paras 6.53 and 6.54 of Ref. [2]).

7.12. If it is discovered that a package has been tampered with during transport, the carrier should notify the relevant authorities and shipper (para. 6.54 of Ref. [2]).

7.13. Once it has been determined that a package is lost, missing, has been stolen or has been tampered with, the carrier should assist the competent authorities and State organizations to locate the package. For example, tracing previous movements and providing any requested information that could assist in identifying the missing package. The carrier should also cooperate with the relevant authorities during subsequent investigations and any prosecutions (para. 6.55 of Ref. [2]).

8. MEASURES FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST SABOTAGE DURING TRANSPORT

8.1. Measures to protect nuclear material against sabotage need to be implemented with due consideration of the impact of such measures on the measures for safety and against unauthorized removal. Most of the measures against unauthorized removal described in Section 6 will also contribute to protecting a shipment against sabotage. Physical protection measures to minimize the potential for a successful act of sabotage may also enhance protection against unauthorized removal, but may complicate operational aspects of transport.

GENERAL APPROACH FOR DESIGNING MEASURES AGAINST SABOTAGE DURING TRANSPORT

Threat assessment and design basis threat

8.2. The State should assess the threats related to the transport of nuclear material and ensure that the threat assessment is kept up to date. Attention should be paid to adversaries with the intention and capability to commit acts of sabotage. These may differ from adversaries with the intention and capability to attempt unauthorized removal. The goal of unauthorized removal is to gain control of intact material for illicit use, whereas the goal of sabotage against a nuclear material shipment is to inflict radiological consequences, or at least the fear of such consequences, on people and the environment. Hence, an act of sabotage might not need to be fully successful to achieve at least part of the goal (paras 3.34 and 3.37 of Ref. [2]).

8.3. In cases where the State issues a design basis threat (DBT), the State may consider issuing a specific DBT related to sabotage. The DBT for sabotage may nevertheless be based on the same assumptions regarding the capabilities of potential adversaries as the DBT for unauthorized removal.

Development of specific threat scenarios

8.4. The DBT for sabotage should incorporate the specific types of action and scenarios that are likely to be followed by saboteurs. In particular, while an unauthorized removal scenario usually comprises two phases — obtaining the material and escaping with the material to make use of it in the future — sabotage typically involves only one phase, defeating the protection of the nuclear material by means of weapons or intrusive tools and creating a radiological hazard. One aspect of a scenario is the number of individuals that could be involved together with their training and experience. A second aspect is the attack methods or modalities they can bring to the scenario to achieve the sabotage objective.

Target identification and ranking

8.5. From a State's perspective, potential targets for sabotage might include any shipment of nuclear material on the territory of the State or carried by a ship or aircraft flagged or registered to the State in international water or airspace. Nevertheless, the State should identify which particular shipments it considers to warrant protection against sabotage, taking account of the capabilities of potential threats and the potential to cause unacceptable radiological

consequences. In doing this, the State should take account of the considerations introduced in paras 4.23–4.25.

8.6. The potential consequences associated with the sabotage of any particular shipment of nuclear material will depend not only upon the activity of the different radionuclides in the nuclear material, but also the physical and chemical form of the material. On this basis, of the materials listed in Table 1, those that may be the most attractive for sabotage are generally irradiated reactor fuel (containing fission product radionuclides) and plutonium. In relation to safety, and to the application of the IAEA Transport Regulations [10] in particular, the radionuclides in such materials present the most significant potential radiological impact and, consequently, the activity limits for their shipment in excepted packages, designated by A_2 , are very low in comparison to other radionuclides. Shipments of irradiated fuel or plutonium may, therefore, involve thousands or millions of times the A_2 value, reflecting the potential consequences that might result from the sabotage of such shipments.

8.7. Other nuclear materials listed in Table 1 have unlimited or relatively large A_2 values, which means that shipments of even large amounts of such material might amount to relatively few times A_2 . Even the total release of such material, if it were possible as a result of sabotage, would produce a limited radiological impact, although the economic and social impacts might nevertheless be substantial.

8.8. Some types of nuclear material pose additional hazards, particularly chemical toxicity. The appropriate competent authority should determine whether such materials warrant particular protection against sabotage.

Estimating the consequences of sabotage considering the threat and the targets: The vulnerability assessment

8.9. The shipper or carrier should seek to minimize the potential impacts of a successful act of sabotage.

8.10. For the targets identified on the basis of the analysis described above, and the threat assessment or DBT, the State or the competent authorities should consider obtaining a quantitative estimate of the potential radiological consequences of a successful act of sabotage by the threat on the targets. This estimation is part of a vulnerability assessment (see also Appendix II).

8.11. Many different potential acts of sabotage could be considered, separately or in combination, in the vulnerability assessment for an attack on a shipment of nuclear material. Some of these acts are relatively sophisticated and might be beyond the capabilities of the threat defined by the State. Others may need a relatively large number of attackers, which also may be beyond the capabilities of the threat. A realistic evaluation of potential threats and their capabilities is an important aspect in undertaking a vulnerability assessment.

8.12. A vulnerability assessment may include the use of both theoretical and numerical tools to assess the potential effect of weapons that an adversary might use on the performance of packages containing nuclear material. The best source of reliable information for such an assessment is specific experiments in which the package is used as a target for the weapon considered to be representative of the DBT (or assumed in the threat assessment). However, such specific information is often not available, and therefore extrapolations and/or arguments from similar cases may be used to provide approximate estimates.

8.13. In assessing the potential effects of sabotage, safety features of the package and conveyance as well as nuclear security measures to prevent unauthorized removal should be taken into account. The structure of the conveyance and the packaging will provide some protection for the nuclear material. The degree of protection provided will depend on the nature of the packaging, which, in turn, will depend on the material being transported. Some nuclear material, such as irradiated nuclear fuel, requires robust heavily shielded packages for safety reasons, and these will also provide substantial protection against sabotage. Other materials, such as uranium, do not require shielded packages and the protection provided by the packaging will be less.

8.14. The vulnerability assessment needs to conclude whether the package safety provisions, such as its shielding walls and containment structure, and the protection measures against unauthorized removal are together sufficient in order to defeat the threat of sabotage. If they are not sufficient, the vulnerability assessment needs to address the extent of damage that could be caused to the package by an act of sabotage and the likely release of radioactive material (activity of the radionuclides released, and their physical and chemical form). In particular, the vulnerability assessment should consider whether the sabotage could result in an unacceptable radiological consequence (as defined by the State).

8.15. Such assessment might be conducted by the shipper or carrier with the support of laboratories specializing in weapons and armour testing. If so, the assessment should be reviewed by the competent authorities as a basis for approval of the shipment and preparation of a shipment contingency plan.

8.16. An act of sabotage involving an explosive device may result in a variety of consequences. These could include:

- (a) Damage due to the blast (generally limited to an area within a few hundred metres from the explosion);
- (b) Dispersal of large particles or pieces of nuclear material (again, generally limited to an area within a few hundred metres from the explosion);
- (c) Airborne dispersal of smaller particles, including respirable particles (potentially affecting an area up to thousands of metres from the explosion, depending on the exact conditions).

8.17. If the vulnerability assessment demonstrates that the package safety provisions and the protection measures against unauthorized removal are not sufficient to defeat the threat of sabotage, an assessment is needed of the amount of radioactive material that could be released by an act of sabotage and the activity of the various radionuclides in that material, including those released in respirable form. This estimate of material released may then be used as a source term for calculation of possible doses to individuals in the vicinity of the shipment in the event of an act of sabotage.

8.18. For any radioactive material, including nuclear material, the main exposure pathways due to a release of the material in an act of sabotage are the same as for any nuclear or radiological emergency [2, 4]:

- (a) Direct radiation dose from unshielded localized material (such as a sealed source);
- (b) Direct radiation dose from dispersed material;
- (c) Internal radiation dose from material that is inhaled during, or shortly after, a successful sabotage event, ingested with food or water contaminated by the release from the sabotage event, or ingested inadvertently owing to contamination of hands.

8.19. The radiological impact is directly linked to the source term released to the environment. The two principal determinants of the amount released from a shipment subjected to sabotage are:

- (a) Radionuclide content of the shipment and of individual packages;
- (b) The fraction of the contents which potentially could be released as a result of the sabotage.

Results and conclusion of the vulnerability assessment

8.20. The source term used for the vulnerability assessment should be compared to the source term used in the development of the contingency plans. If the potential release of activity due to an act of sabotage is within the source term used in the definition of the current contingency plan, then it may be concluded that this plan and the protective measures outlined in the TSP are also sufficient for a sabotage scenario, although specific considerations for possible cases of sabotage may still need to be taken into account by the response teams (see Section 9).

8.21. If the vulnerability assessment demonstrates that the sabotage event could result in unacceptable radiological consequences, then consideration should first be given to amending the protection measures in the TSP. In addition, the contingency plan might need to be revised, taking into account this new source term resulting from sabotage and establishing modified measures based on it.

8.22. Appropriate dose criteria, consistent with the guidance in IAEA Safety Standards Series No. GSG-2, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency [6], should be defined at which protective and other response actions are planned to be taken immediately to prevent severe radiological effects in the event of a nuclear emergency resulting from sabotage of nuclear material in transport. Operational criteria derived from these dose criteria will be one of the principal determinants of the level of effort planned to reduce the potential radiological impacts of a successful sabotage event affecting nuclear material in transport (see GSG-2 [6]).

8.23. Revision of the contingency plan, based on the results of the vulnerability assessment approved by the competent authorities, should be undertaken with those entities involved in developing the contingency plan.

8.24. Alternatively, it may be possible to add additional mitigating features to the transport package or its conveyance, as described in paras 8.26–8.31, to reduce the potential release to an acceptable level. However, this should not remove the need to have arrangements in place to respond to an emergency involving the nuclear material in transport, in accordance with the safety requirements in IAEA Safety Standards Series No. GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency [8].

DEFINING PHYSICAL PROTECTION MEASURES AGAINST SABOTAGE

8.25. Paragraphs 8.26–8.31 apply to the carrier and/or the shipper, whichever is responsible for implementing additional measures to protect nuclear material against sabotage.

Applicable physical protection measures

8.26. A wide variety of measures could be applied to existing packaging for nuclear material in order to reduce the release of radioactive materials in the event of sabotage of the shipment. Several of these measures could also contribute to preventing the unauthorized removal of the material by increasing the time needed to extract the material from the packaging.

8.27. Possible measures include protecting against an attack using a device placed close to the package/conveyance, providing a sufficient delay or preventing access to the package, or preventing visual observation of the package. Measures to reduce the effects of explosives or the penetration of missiles could be considered.

8.28. Such measures may affect the operation of the transport system, because additional procedures may be needed in preparing a shipment, but the measures should not adversely affect the safety of the package.

Applicable organizational measures

8.29. During loading, unloading and transfer, when packages must be removed from their conveyances, the State should consider the need for compensatory protective measures such as additional guards, barriers and surveillance.

8.30. Operational measures might include routing changes to avoid areas where the radiological and/or economic consequences of a successful sabotage event might be particularly high.

8.31. If a review of the physical protection measures indicates that they are not sufficient to counter the current threat of sabotage, the State may consider postponing the shipment.

9. MEASURES TO MITIGATE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE DURING TRANSPORT

9.1. In addition to being prepared to respond to an act or attempted act of unauthorized removal of nuclear material in transport, the State should be prepared to respond to an act of sabotage. An act of sabotage may result in radiological consequences that need to be mitigated to reduce the impact on people and the environment. The security of the shipment should be maintained during such a response, and careful planning and coordination between security and safety response forces is therefore needed (para. 6.60 of Ref. [2]).

9.2. The radiological consequences of an act of sabotage are likely to be similar in many respects to those of a severe transport accident that results in a release of the radioactive contents of the packages. However, in the case of an act of sabotage, there may be additional casualties, and the security of the scene of the event needs to be maintained for the continued protection of the cargo and preservation of evidence that may be needed for criminal investigations.

9.3. Detailed guidance on planning and preparing for accidents during the transport of radioactive material, and generally on response to nuclear and radiological emergencies (whether these result from accidents or malicious acts) is provided in other IAEA publications [6–8].

RESPONSIBILITIES

9.4. If an act of sabotage involving nuclear material occurs during transport, several governmental organizations, the shipper, the carrier and the guards, escorts and security response personnel have a responsibility to act to mitigate its consequences. This response may include providing medical treatment and

saving lives, suppressing or controlling fires, securing the area to ensure the physical protection of the nuclear material, and actions associated with possible subsequent criminal investigations. In addition, consideration should be given to calling in specialized organizations trained to deal with radioactive material to assess the event and help to implement the measures used to contain, control or eliminate any radiological hazard in accordance with the requirements in GS-R-2 [8]. The degree of involvement of the various organizations may vary during the progress of the operation.

9.5. The responsibilities for planning and implementing a response to an act of sabotage are generally divided among several involved organizations and persons. The severity of the event and the characteristics of the nuclear material involved (including the potential radiological consequences) generally determine the level of governmental response. The governmental responsibilities and responses depend on the legal framework of the State concerned and may therefore differ from State to State. Designation within the State of a ‘national coordinating authority’ as a focal point may be useful for developing and coordinating governmental response plans for acts of sabotage involving shipments of nuclear material. This may also be useful for coordinating the development of national, provincial and local emergency response plans, and facilitating proper emergency preparedness. The State should clearly define the roles and responsibilities of all governmental levels (local, provincial and national), and of shippers and carriers.

9.6. The carrier and the shipper should be prepared to respond to an act of sabotage and provide the appropriate technical assistance to emergency responders and security response forces. The shipper or carrier should ensure that adequate arrangements are available to initiate a State response to deal effectively with any radiological consequences of such an act. These arrangements may include being prepared to provide information about the shipment and providing emergency and/or technical assistance when requested or required.

PLANNING

9.7. The State should establish a contingency plan that includes acts of sabotage during the transport of nuclear material. This overall plan should provide the basis for contingency plans prepared by shippers and/or carriers. The State should ensure that relevant entities conduct exercises — including joint exercises — to assess and validate the elements of the contingency plan related to acts of sabotage (paras 6.62, 6.63, 6.66 and 6.68 of Ref. [2]).

9.8. 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 (para. 6.65 of Ref. [2]).

9.9. The State should develop and provide guidance for personnel that might be involved in response to an act of sabotage with radiological consequences in accordance with the requirements and guidance in GSG-2 [6] and GS-R-2 [8]. For example, police and fire personnel should be aware of basic radiation protection measures and the actions they should take. Such guidance may build on existing guidance that covers procedures and measures to be taken in the event of a transport accident that involves possible radioactive material release [21].

CARRIER ACTIONS

9.10. The carrier should ensure that its personnel are fully trained and prepared to act in full coordination with guards, response forces and law enforcement agencies in the event of an act of sabotage or other activation of the contingency plan (para. 6.70 of Ref. [2]).

9.11. In the event of an act of sabotage, the carrier or other designated personnel accompanying the shipment should immediately initiate the actions set out in the contingency plan. The carrier or other designated personnel should also notify the transport control centre or the management of the carrier as specified in the contingency plan (para. 6.72 of Ref. [2]).

9.12. Immediately following any act of sabotage, the carrier or other designated personnel and/or guards should take measures to secure the nuclear material, the scene of the event and the conveyance. Measures to reduce the consequences of the act should also be taken as specified in the contingency plan (para. 6.73 of Ref. [2]).

Appendix I

THE TRANSPORT SECURITY PLAN

I.1. An example structure of a transport security plan (TSP) for use with the performance based approach is provided in Box 1. A State may need to modify this outline to reflect its own particular circumstances, but the example contains all of the information that the State needs in order to validate and approve the transport activities of those who propose to transport nuclear material. States should require this structure or a structure similar to this to facilitate understanding between shippers, carriers, receivers and regulators, both domestically and internationally.

I.2. For information security reasons, the State may require that the TSP be developed in the form of a series of separate documents, each of which may be provided only to those that need to know those parts of the plan.

I.3. In addition, since in the performance based approach the entity responsible for preparing and submitting the TSP has access to knowledge from the State's threat assessments or DBT, enhanced protection of the information in the TSP or elements thereof may be needed.

I.4. For the prescriptive approach, the listing of provisions required by the competent authorities should be inserted in section 1.2.2 of the example structure in Box 1.

I.5. The following sections outline the details that should be considered for inclusion in a TSP for a shipment undertaken following the performance based approach. If the entity responsible for preparing and submitting the TSP is required by the competent authorities to apply the performance based or combined approach, a vulnerability assessment may be required (see Appendix II).

ADMINISTRATIVE REQUIREMENTS AND INFORMATION

I.6. This section should include the complete legal name and address of the entity responsible for preparing and submitting the TSP, plus all appropriate telephone, fax and email addresses of those who are applying for approval of the TSP. This should include information about the shipper, carriers or others who might be involved with the proposed shipment, including guards employed

BOX 1: EXAMPLE STRUCTURE OF THE TRANSPORT SECURITY PLAN FOR THE PERFORMANCE BASED APPROACH

1. ADMINISTRATIVE REQUIREMENTS AND INFORMATION
 - 1.1. Allocation of responsibilities
 - 1.2. Policies and operational procedures
 - 1.2.1. Vulnerability assessment
 - 1.2.2. Testing and evaluation of the transport security plan
 - 1.2.3. Review and update of the transport security plan
 - 1.2.4. Response to higher threat conditions
 - 1.2.5. Reporting of threats or incidents
 - 1.3. Training requirements
 - 1.4. Information management
 - 1.4.1. Retention of records
 - 1.4.2. Confidentiality and protection of information
 - 1.5. Trustworthiness of personnel
2. SHIPMENT SECURITY
 - 2.1. Description of the nuclear material to be transported
 - 2.2. Description of the transport physical protection system
 - 2.2.1. Packages and conveyances
 - 2.2.2. Planned and alternative routes and modes of transport
 - 2.2.3. Physical protection measures
 - 2.2.4. Communications and positional tracking for normal operations
 - 2.2.5. Command and control for normal operations
 - 2.3. Maintenance and testing of systems and equipment
 - 2.4. Pre-shipment checks
3. RESPONSE PLANNING
 - 3.1. Emergency arrangements
 - 3.2. Contingency plans
 - 3.2.1. Guards
 - 3.2.2. Response forces
 - 3.3. Incident communications, command and control

for the shipment, and information about the receiver and transit States when international transport is proposed. It should also contain detailed information in subsections as elaborated in the following.

Allocation of responsibilities

I.7. The TSP should clearly establish responsibility for each of the provisions and measures specified therein. It should identify all involved personnel who have the appropriate authority to carry out their responsibilities, and should clearly specify who — the shipper, carrier or receiver — has direct responsibility for the security of the nuclear material during each particular mode or phase of the transport. Whenever responsibility for a shipment is to be changed from one party to another (e.g. between carriers at a national border, or between a carrier or receiver, or a facility operator when the shipment is being placed into in-transit storage), the transfer of responsibilities should be specified.

I.8. If any transport activities are subcontracted, the TSP should identify all contractual arrangements that will be needed to develop and comply with the TSP.

Policies and operational procedures

I.9. Relevant policies and operational procedures should be clearly documented in this section of the TSP, including detailed measures to implement policies (e.g. policies on response procedures for higher threat conditions and employment verification for new staff), operating practices (e.g. choice and use of routes where known, use of guards and access to nuclear material packages at temporary storage facilities en route), and equipment and resources that are to be used to reduce security risks.

Vulnerability assessment

I.10. For the performance based approach, and some variants of the combined approach, the administrative and technical requirements specified in the State's regulatory framework should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment. The competent authorities may require the entity responsible for preparing and submitting the TSP to prepare a vulnerability assessment (see Appendix II).

Testing and evaluation of the transport security plan

I.11. The TSP should specify the procedures for evaluating and testing it.

Review and update of the transport security plan

I.12. The TSP should be reviewed periodically, and updated when necessary, to ensure that the latest information available to the State relevant to the security of nuclear material shipments is taken into account. The TSP should specify when and how such reviews and updates are to be conducted.

Response to higher threat conditions

I.13. As required by the competent authorities, the TSP should be evaluated periodically to ensure that the most recent threat information is taken into account. Should the State designate that a higher threat condition exists at the time the shipment is to be undertaken than was assumed in developing the current TSP, appropriate actions should be taken to address this higher threat condition and a revised TSP should be developed.

Reporting of threats or incidents

I.14. The TSP should require that any incidents or unscheduled delays that occur during transport be documented by the carrier and reported, within a specified time, to the shipper, receiver and, if applicable, the competent authorities. The TSP should also specify that a review of physical protection arrangements should be undertaken after a shipment is completed in order to evaluate the effectiveness of the TSP and to identify any necessary improvements which may be made to improve its effectiveness for future shipments.

Training requirements

I.15. This section of the TSP should identify the training that will be conducted and the exercises that will be arranged, and specify the schedule that will be followed for each (since the State competent authorities or equivalent bodies may wish to witness the exercises). The training and exercises should address all appropriate aspects of physical protection, including for the management of organizational interfaces and specified functions for emergency response. Arrangements should be made for the results of exercises to be systematically evaluated by the participating organizations and, as appropriate, by the appropriate State competent authority. The results of all training exercises should

be documented, and any corrective actions identified during the process should be implemented promptly.

Information management

I.16. The TSP should clearly define the measures to be taken to protect the confidentiality of information deemed sensitive or classified by the competent authorities. Information management procedures should ensure that the distribution of sensitive transport information is limited to appropriate individuals on a need to know basis. Such measures should not preclude the proper application of provisions needed in transport documents and shippers' declarations as required by the IAEA Transport Regulations [10].

Retention of records

I.17. This section of the TSP should address how the records of nuclear material shipments, including details of the packages used and the nuclear material they contained, and information on the personnel involved in the shipment, should be maintained and updated as necessary, consistent with requirements specified by the competent authorities. In addition, records should be maintained of all nuclear material that has been transported through the State. Records associated with the preparation and actual undertaking of a shipment, including the training and qualification of personnel, should be retained in a manner and for a time period that is consistent with that specified by the State.

Confidentiality and protection of information

I.18. This section of the TSP should describe measures to be taken, consistent with national requirements, to protect the confidentiality of information relating to transport operations. These measures should include protecting detailed information on the type, category and quantity of the nuclear material, the schedule, route and timings of the shipment, physical protection arrangements, and the number, names and qualifications of personnel involved in the shipment. Particular consideration should be given to those operations involving Category I and II nuclear material.

I.19. The TSP will itself contain sensitive information on aspects of the shipment, including details of the packages and conveyances used to transport the material. Thus, the TSP should be handled in such a way as to protect the confidentiality of such information in accordance with the applicable provisions of the State. The entity responsible for preparing and submitting the TSP should follow the

provisions determined by the State, taking all necessary precautions to prevent unauthorized access to any sensitive information contained in the TSP.

Trustworthiness of personnel

I.20. This section of the TSP should specify how the trustworthiness of individuals involved in the proposed shipment will be verified. All persons receiving advance knowledge of transport information regarding Category I, II and III nuclear material should be subject to trustworthiness verification commensurate with the provisions specified by the State and with their assigned responsibilities. The trustworthiness verification should be completed before such information is transmitted to those persons and this information should be appropriately classified and protected as required by the State.

SHIPMENT SECURITY

I.21. Operating practices should identify equipment and resources that are to be used to reduce security risks. Such operating practices should be described in the TSP, including:

- (a) Choice and use of routes, where known, including identification of safe havens;
- (b) Use of guards;
- (c) Engineered systems to be used to enhance security;
- (d) Limiting access to nuclear material packages requiring the enhanced security level while in temporary storage en route.

I.22. This section of the TSP should include a general discussion of these practices, and specific subsections as follows.

Description of the nuclear material to be transported

I.23. This section of the TSP should include information on the type of the nuclear material (i.e. plutonium, ^{233}U , ^{235}U or irradiated fuel), its category (i.e. Category I, II or III), the amount of nuclear material and its physical and chemical form, the isotopic composition and enrichment level, radiation levels and any other applicable data (e.g. age and burnup of irradiated fuels).

Description of the transport physical protection system

I.24. This section of the TSP should describe the manner in which all of the elements that constitute the physical protection system for the transport of nuclear material are designed and maintained.

Packages and conveyances

I.25. This section of the TSP should identify the packages to be used and any information on these designs that is pertinent to nuclear security. If specially designed conveyances are to be used, they should be described along with any protective capabilities those conveyances might provide (in terms of deterrence, detection and/or delay).

Planned and alternative routes and modes of transport

I.26. This section of the TSP should contain a detailed description of the planned modes of transport and the planned primary routes to be followed, and all available information on these routes that would be useful to the State authorities, competent authorities, carrier personnel, guards and response forces.

I.27. This information should include, as applicable, current conditions that could affect the shipment: on relevant roads, railways and inland waterways; at port facilities, transfer and stopover facilities; at border crossings and airports. It includes:

- (a) Permissible speeds;
- (b) Areas where repair or construction work is being, or is expected to be, performed;
- (c) Potential weather conditions;
- (d) Capabilities at planned transfer points and stopover facilities;
- (e) Locations of refuelling sites;
- (f) Potential safe havens and subsistence locations.

I.28. Alternative routes that could be used in case of unforeseen circumstances should also be identified and described, including expected conditions on those routes and information similar to that reported for the proposed primary routes.

Physical protection measures

I.29. This section of the TSP should describe how the shipper or carrier has designed its physical protection system to accomplish the objectives of deterrence, detection, assessment, delay and response. This section of the TSP should describe the physical protection measures that are proposed, recognizing that ensuring security during the transport of nuclear material is, in many ways, more challenging than at a nuclear facility. For example, it is difficult, if not impossible, to entirely preclude public access to shipments being made in public areas. Furthermore, an attempt at unauthorized removal, sabotage or other nuclear security related incident could occur anywhere along a transport route, which may extend over a significant distance and include remote areas, thereby giving an adversary a wide choice of potential attack locations. At some locations, it may be particularly difficult for adequate response forces to arrive within a useful period of time, in which case alternative response forces would need to follow the transport convoy at a reasonable distance.

Communications and positional tracking for normal operations

I.30. This section of the TSP should describe the structure of the primary and alternative communications systems for the proposed transport operation. Any system proposed to be used for tracking the conveyances should be described. Such a system should be located at, and operated by, a transport control centre or an alternative central point of communication if one is required by the competent authorities. Alternative communications systems, when required, should not be vulnerable to the same failure mode as the primary system in order to ensure at least one means of communication is available at all times.

Command and control for normal operations

I.31. This section of the TSP should describe command and control procedures and designate the persons of authority for each phase of the transport operation. It should address the entire command and control arrangement for the shipment and define how it is coordinated with the communications structure and procedures. It should describe command and control procedures, designating the responsible authority and appropriate chain of command for each phase of the transport operation, making clear who has authority to make critical decisions for each phase, for routine situations or for response to an emergency or nuclear security event. When guards are used, the TSP should also define command and coordination procedures between the response forces and the guards, and

between the primary response forces and any secondary response forces that may be planned for deployment.

I.32. The chain of command should be described clearly and simply, and should define who has the authority to give the final decision to start, delay, cancel or interrupt the transport operation, and to take action in the event of an emergency or nuclear security event. It should specifically define the roles and responsibilities of the transport commander, the response force commander and the transport control centre, and should specify how and when transfer of command and control would be made from the transport commander to the response force commander if this were to be necessary.

Maintenance and testing of systems and equipment

I.33. This section of the TSP should address the manner in which all of the systems involved in the shipment are designed and maintained.

I.34. The section should also describe the inspection and testing of all equipment related to the shipment, to be performed prior to the beginning of the transport operations. Categories of equipment that should be inspected and tested before the commencement of a shipment include:

- (a) All transport conveyances;
- (b) Communications equipment and tracking systems;
- (c) Any delay systems (e.g. personnel barriers, vehicle immobilization systems) built into the transport packages or conveyances;
- (d) Weapons, tactical and protective equipment, and communication devices of guards and response forces.

Pre-shipment checks

I.35. This section of the TSP should describe the competent authorities' requirements and the shipper's or carrier's arrangements for pre-shipment checks or readiness reviews.

RESPONSE PLANNING

Emergency arrangements³

I.36. This section of the TSP should address planned actions and procedures in the event of an emergency situation, such as a road closure, vehicle breakdown, vehicle accident or driver illness, that may occur during shipment. Emergency arrangements include, but are not limited to, availability of a backup vehicle and driver, capability for heavy towing and lifting, and plans for use of safe havens and alternative routes.

I.37. This section should also address the need and capability to immediately inform any transport control centre or alternative central point of communication of any emergency situation, and for that control centre or central point to be able to initiate the planned actions and/or procedures in response.

Contingency plans

I.38. The TSP should designate specific individuals who have the responsibility and authority to carry out contingency plans if a nuclear security event occurs.

I.39. This section should also address the capability to ensure that any transport control centre or alternative central point of communication can be made immediately aware of a nuclear security event and the time and place that it started. It should also address planned actions and procedures to be taken by the control centre or alternative central point of communication should a nuclear security event occur.

I.40. The contingency plan should include procedures, such as the employment of guards and response forces, which will provide depth to the defences used during shipment. It should therefore identify:

- (a) Any guards that are designated to accompany the shipment;
- (b) All response force units or organizations that are assigned responsibilities for the shipment;
- (c) Any other State assets that are projected to be available to support the shipment or assist in response to an incident or emergency;

³ This section refers to actions and procedures in the case of non-nuclear emergency situations and should not be confused with arrangements for response to a nuclear or radiological emergency.

- (d) All other support personnel, including fire, rescue and other services along the route, as applicable, and the communications system to be used to communicate with them.

Guards

I.41. A graded approach should be used in deciding on the use of guards, and this should be reflected in the TSP. For example, the competent authorities may determine that the use of guards should be considered to accompany shipments of Category III nuclear material, whereas it should require guards to accompany shipments of Category I and II nuclear material. If armed guards are used, rules for the use of firearms should be clearly documented. If guards do not accompany the shipment, then the driver or operator of the conveyance, or another designated crew member, should be capable of providing surveillance of the nuclear material and of making any required notifications in the event of an attack or adverse conditions, in accordance with the information provided in the shipper's or carrier's TSP.

Response forces

I.42. The TSP should specify how the shipper or carrier will maintain and have readily available, to the extent possible, accurate information on the availability and capability of potential local response forces (e.g. local law enforcement personnel) close to the route chosen.

Incident communications, command and control

I.43. This section of the TSP should describe command and control procedures and arrangements, and communications structure and procedures, additional to those for normal operations, to be applied in an emergency situation.

Appendix II

THE VULNERABILITY ASSESSMENT

II.1. For the performance based approach and some variants of the combined approach, the administrative and technical requirements specified in the TSP should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment.

II.2. If required by the State, the TSP should specify that the review of current or proposed transport operations and assessment of vulnerability will be conducted as appropriate, and that the resulting vulnerability assessment will be appropriately documented and used by the shipper, carrier or responsible authority in developing its physical protection measures.

II.3. The competent authorities may require that a vulnerability assessment be performed for the whole TSP or any part thereof that it considers warrants more detailed analysis, such as stopping points, route selection and transfer points. The vulnerability assessment may be a separate document classified appropriately and referenced in the TSP. The entity responsible for preparing and submitting the vulnerability assessment might not be the same entity responsible for preparing the TSP.

II.4. The assessment of the performance of any security system needs a methodical approach in which the ability of the system to meet stated requirements is determined.

II.5. The vulnerability assessment process comprises three major phases: planning the assessment, conducting it and concluding it.

PLANNING THE VULNERABILITY ASSESSMENT

II.6. A realistic evaluation of potential threats and their capabilities is an important aspect in undertaking a vulnerability assessment. In most cases, a vulnerability assessment will be a sufficiently complex process that explicit, detailed planning is needed to help to ensure that the assessment includes all necessary considerations, and that the objectives are met. The planning phase includes the following activities.

Establishing the scope and objectives of the vulnerability assessment

II.7. In the initial planning phase, it is necessary to determine the scope and objectives of the vulnerability assessment. Reference should also be made at this stage to relevant threat assessments and/or the DBT and to any constraints.

II.8. The scope of work should clearly define all expected deliverables and indicate the complexity and rigour with which the assessment should be conducted. The complexity and rigour of the assessment will depend on:

- (a) The nature of the shipment, including the characteristics of the nuclear material;
- (b) The threat environment at the proposed time of shipment;
- (c) The time available to complete the assessment.

II.9. During transport, vulnerability may change dramatically at the different stages of the transport operation, for different modes of transport and for different routes.

Selecting knowledgeable team members, and defining roles and responsibilities

II.10. A team of experts may be created to ensure that a complete and accurate vulnerability assessment is produced. The team should include security specialists who can ensure that the vulnerability assessment is correct. The members of the team should collectively have knowledge of all of the main topics relevant to the vulnerability assessment, including physical protection systems, response actions, data analysis and managing radioactive contamination.

Developing a schedule with deliverables and resource requirements

II.11. When developing the schedule, consideration should be given to setting a realistic time frame for the assessment and to any foreseeable risks that might prevent achievement of the objectives. All team members should be consulted to determine the resources needed to achieve the required results in the allotted time.

CONDUCTING THE VULNERABILITY ASSESSMENT

II.12. The process steps within the second phase of a vulnerability assessment are:

- (a) To state the objectives of the physical protection system;
- (b) To describe the components of the physical protection system;
- (c) To characterize the components of the physical protection system;
- (d) To analyse the ability of the physical protection system to meet the objectives.

Stating the objectives of the physical protection system

II.13. The vulnerability assessment starts with a statement of the objectives of the physical protection system for the shipment as provided by the competent authorities. This section may include relevant aspects of the DBT or threat assessment (if confidentiality considerations allow).

Describing the components of the physical protection system

II.14. The tasks to be completed during this step of a vulnerability assessment include a description of the components of the physical protection system, the transport system, the nuclear material to be transported and, where applicable, the response forces.

II.15. A description of the transport system is important for establishing operational, safety and physical constraints on the physical protection system, as well as mode specific requirements. Understanding the material to be transported is important for applying a graded approach based on potential consequences of a malicious act and establishing performance requirements for the physical protection systems (preferably established by a separate consequence based risk analysis). The description of the response forces, if included, should include information on weapons, tactics and training.

II.16. This section should include applicable information on all phases of the proposed shipment, such as any planned intermodal transfer operations, temporary in-transit storage and sections of routes that pass through high and low population areas.

Characterizing the components of the physical protection system

II.17. Characterization of a physical protection system involves gathering data, and often includes the development and validation of models, to determine how the human, procedural and technological elements of a physical protection system may be expected to perform against attack as postulated in the DBT or the threat assessment. In general, these elements are evaluated in terms of the ability to defeat an adversary, as effects of deterrence are difficult to quantify. Defeating an adversary may be broken down into the nuclear security functions of detection, assessment, delay and response. The measures used to characterize performance in respect of these security functions should support the input requirements for the analysis techniques to be used in the following performance determination step. Performance data are gathered by conducting tests at the component and element level.

Analysing the ability of the system to meet the objectives

II.18. This step of the vulnerability assessment is to determine the performance of the physical protection system in meeting the objectives in relation to the threat. System models may be used and may be predictive or schematic in nature, and qualitative or quantitative. The goal of using such models is to predict how the physical protection system, as currently operating or proposed, will perform against the DBT or other defined threat. System models, or at least models of particular scenarios, may be validated through appropriate exercises, such as table top exercises, simulations and force-on-force exercises.

CLOSURE OF THE VULNERABILITY ASSESSMENT

II.19. The last phase of a vulnerability assessment has the goal of providing an accurate record of the assessment. This should include descriptions of the methodology used, the assumptions made, the data collected and the results on the effectiveness of the physical protection system. The form in which the results are reported should be usable by those responsible for making decisions regarding the adequacy of the physical protection system evaluated. The reporting of results is typically conducted by two methods: briefings and written reports.

II.20. If the vulnerability assessment concludes that the physical protection system does not meet the established objectives, the documentation should include recommendations concerning potential solutions. Such solutions should be based on insights gained during the conduct of the vulnerability assessment and not on a detailed assessment of various design options. While the members of a vulnerability assessment team may be given responsibility for developing design recommendations in addition to conducting the vulnerability assessment itself, this should be considered a design upgrade activity and not an assessment of an existing physical protection system. On review of the results, the competent authorities and shippers or carriers may consider providing additional information to improve the scope or accuracy of the assessment in order to address apparent disparities between security system requirements and performance projections. Because performance requirements are often based on risk assessments, changes in the material being transported (e.g. quantity) will alter the potential consequences of theft or sabotage, and thus may alter the conclusions of the assessment.

II.21. If the competent authorities consider that the State's requirements are not met by the vulnerability assessment or the assessment is otherwise inadequate, it should be returned to the originator for additional information and modification.

REFERENCES

- [1] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
- [3] Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
- [5] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE, ORGANIZATION-INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).
- [6] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).
- [7] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).
- [8] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material (2012 Edition), IAEA Safety Standards Series No. SSR-6, IAEA, Vienna (2012).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Preparing for Emergency Response to Transport Accidents Involving Radioactive Material, IAEA Safety Standards Series No. TS-G-1.2 (ST-3), IAEA, Vienna (2002).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
- [13] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Technical Instructions for the Safe Transport of Dangerous Goods by Air, ICAO Doc 9284, ICAO, Montreal (2014).
- [14] INTERNATIONAL MARITIME ORGANIZATION, IMDG Code: International Maritime Dangerous Goods Code, 2014 edn, 2 vols, IMO, London (2014).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
- [16] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, International Maritime Organization, London (1988).
- [17] International Convention for the Safety of Life at Sea (as amended), International Maritime Organization, London (1974).
- [18] INTERNATIONAL MARITIME ORGANIZATION, International Ship and Port Facility Security Code, IMO, London (2004).
- [19] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Convention on International Civil Aviation, ICAO Doc 7300/9, ICAO, Montreal (2006).
- [20] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Annex 17 to the Convention on International Civil Aviation — Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference, 9th edn, ICAO, Montreal (2011).
- [21] INTERNATIONAL ASSOCIATION OF FIRE AND RESCUE SERVICES, INTERNATIONAL ATOMIC ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Manual for First Responders to a Radiological Emergency, EPR-First Responders 2006, IAEA, Vienna (2006).

GLOSSARY

carrier. Any person, organization or government undertaking the carriage of nuclear material by any means of transport. The term includes both carriers for hire or reward (known as common or contract carriers in some States) and carriers on own account (known as private carriers in some States).

competent authority. A governmental organization or institution that has 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 nuclear security 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 nuclear security measures proportionate 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.

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.

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

nuclear facility. A facility (including associated buildings and equipment) at 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 a means to support, enhance and sustain nuclear security.

nuclear security event. An event that has potential or actual implications for nuclear security that must be addressed.

operator. Any person, organization or government entity licensed or authorized to undertake the operation of an associated facility or to perform an associated activity.

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 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; and 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.

shipment. The specific movement of a consignment (nuclear material) from origin to destination.

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

source term. The amount and isotopic composition of radioactive material released (or postulated to be released) following sabotage.

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 transport, 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.

unacceptable radiological consequences. A level of radiological consequences, established by the State, above which the implementation of nuclear security measures is warranted.

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



ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

BELGIUM

Jean de Lannoy

Avenue du Roi 202, 1190 Brussels, BELGIUM

Telephone: +32 2 5384 308 • Fax: +32 2 5380 841

Email: jean.de.lannoy@euronet.be • Web site: <http://www.jean-de-lannoy.be>

CANADA

Renouf Publishing Co. Ltd.

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA

Telephone: +1 613 745 2665 • Fax: +1 643 745 7660

Email: order@renoufbooks.com • Web site: <http://www.renoufbooks.com>

Bernan Associates

4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA

Telephone: +1 800 865 3457 • Fax: +1 800 865 3450

Email: orders@bernan.com • Web site: <http://www.bernan.com>

CZECH REPUBLIC

Suweco CZ, s.r.o.

SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC

Telephone: +420 242 459 205 • Fax: +420 284 821 646

Email: nakup@suweco.cz • Web site: <http://www.suweco.cz>

FRANCE

Form-Edit

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE

Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90

Email: fabien.boucard@formedit.fr • Web site: <http://www.formedit.fr>

Lavoisier SAS

14 rue de Provigny, 94236 Cachan CEDEX, FRANCE

Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02

Email: livres@lavoisier.fr • Web site: <http://www.lavoisier.fr>

L'Appel du livre

99 rue de Charonne, 75011 Paris, FRANCE

Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80

Email: livres@appeldulivre.fr • Web site: <http://www.appeldulivre.fr>

GERMANY

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen

Willstätterstrasse 15, 40549 Düsseldorf, GERMANY

Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28

Email: s.dehaan@schweitzer-online.de • Web site: <http://www.goethebuch.de>

HUNGARY

Librotrade Ltd., Book Import

Pesti ut 237. 1173 Budapest, HUNGARY

Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274

Email: books@librotrade.hu • Web site: <http://www.librotrade.hu>

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA

Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928

Email: alliedpl@vsnl.com • Web site: <http://www.alliedpublishers.com>

Bookwell

3/79 Nirankari, Delhi 110009, INDIA

Telephone: +91 11 2760 1283/4536

Email: bkwell@nde.vsnl.net.in • Web site: <http://www.bookwellindia.com>

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY

Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48

Email: info@libreriaaeiou.eu • Web site: <http://www.libreriaaeiou.eu>

JAPAN

Maruzen Co., Ltd.

1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN

Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160

Email: journal@maruzen.co.jp • Web site: <http://maruzen.co.jp>

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION

Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59

Email: secnrs@secnrs.ru • Web site: <http://www.secnrs.ru>

UNITED KINGDOM

The Stationery Office Ltd. (TSO)

St. Crispins House, Duke Street, Norwich, NR3 1PD, UNITED KINGDOM

Telephone: +44 (0) 333 202 5070

Email: customer.services@tso.co.uk • Web site: <http://www.tso.co.uk>

UNITED STATES OF AMERICA

Bernan Associates

4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA

Telephone: +1 800 865 3457 • Fax: +1 800 865 3450

Email: orders@bernan.com • Web site: <http://www.bernan.com>

Renouf Publishing Co. Ltd.

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA

Telephone: +1 888 551 7470 • Fax: +1 888 551 7471

Email: orders@renoufbooks.com • Web site: <http://www.renoufbooks.com>

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, 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>

**OBJECTIVE AND ESSENTIAL ELEMENTS
OF A STATE'S NUCLEAR SECURITY REGIME****IAEA Nuclear Security Series No. 20**

STI/PUB/1590 (15 pp.; 2013)

ISBN 978-92-0-137810-1

Price: €20.00

**NUCLEAR SECURITY RECOMMENDATIONS
ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL
OUT OF REGULATORY CONTROL****IAEA Nuclear Security Series No. 15**

STI/PUB/1488 (33 pp.; 2011)

ISBN 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 (27 pp.; 2011)

ISBN 978-92-0-112110-3

Price: €22.00

**NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL
PROTECTION OF NUCLEAR MATERIAL AND
NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)****IAEA Nuclear Security Series No. 13**

STI/PUB/1481 (57 pp.; 2011)

ISBN 978-92-0-111110-4

Price: €28.00

SECURITY IN THE TRANSPORT OF RADIOACTIVE MATERIAL**IAEA Nuclear Security Series No. 9**

STI/PUB/1348 (39 pp.; 2008)

ISBN 978-92-0-107908-4

Price: €20.00

This publication provides guidance to States and their competent authorities on how to implement and maintain a physical protection regime for the transport of nuclear material. It may also be useful to shippers or carriers of nuclear material in the design and implementation of their physical protection systems.

This publication builds upon the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, and provides additional guidance on how to implement these recommendations in practice.

**INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA**

ISBN 978-92-0-102015-4

ISSN 1816-9317