IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

No. 46-T

Security of Nuclear and Other Radioactive Material in Transport

TECHNICAL GUIDANCE

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 AND OTHER RADIOACTIVE MATERIAL IN TRANSPORT

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 46-T

SECURITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL IN TRANSPORT

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
tel.: +43 1 2600 22529 or 22530
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
November 2024
STI/PUB/2090
https://doi.org/10.61092/iaea.4umu-2uji

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Security of nuclear and other radioactive material in transport / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 46-T | Includes bibliographical references.
Identifiers: IAEAL 24-01703 | ISBN 978-92-0-117424-6 (paperback : alk. paper) | ISBN 978-92-0-117524-3 (pdf) | ISBN 978-92-0-117624-0 (epub)
Subjects: LCSH: Radioactive substances — Transportation. | Radioactive substances — Security measures. | Radioactive substances — Safety measures.
Classification: UDC 656.073 | STI/PUB/2090

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

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.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance to States in order to assist them in implementing and reviewing their national nuclear security regimes, and in strengthening these regimes when necessary. The series also provides guidance to help States to fulfil their obligations and commitments with respect to binding and non-binding international instruments adopted under the auspices of the IAEA or other organizations.

1.2. IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [1], provides recommendations on the physical protection of nuclear material in use, storage and transport. IAEA Nuclear Security Series No. 26-G, Security of Nuclear Material in Transport [2], provides detailed guidance on how to implement those recommendations in order to assist States' competent authorities and shippers or carriers[1] in fulfilling their responsibilities regarding the physical protection of nuclear material in transport.

1.3. IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3], provides recommendations for the security of radioactive material throughout the life cycle of the material, including during transport. IAEA Nuclear Security Series No. 9-G (Rev. 1), Security of Radioactive Material in Transport [4], provides guidance on establishing transport security levels for radioactive material in transport and for establishing security measures against the unauthorized removal and sabotage of radioactive material in transport.

1.4. Also relevant to the present publication are the revised Recommendations on the Transport of Dangerous Goods [5] (also referred to as Model Regulations), issued by the United Nations Economic Commission for Europe to help States to develop security requirements for the transport of all dangerous goods.[2]

---

[1] In this publication, the term 'shipper or carrier' refers to the entity to which any specific physical protection responsibility related to transport is assigned.

[2] Provisions related to the transport of radioactive material are given in Chapters 1.4, 1.5 and 7.2 of the Model Regulations [5].

1.5. Other specialized agencies and programmes of the United Nations have taken steps to support improved security in the transport of dangerous goods during specific modes of transport. The International Maritime Organization, the International Civil Aviation Organization, the United Nations Economic Commission for Europe and the Intergovernmental Organization for International Carriage by Rail have all amended their respective international instruments [6–10] to reflect the security provisions of the Model Regulations [5].

1.6. The Convention on the Physical Protection of Nuclear Material [11] and its Amendment [12] provide an international framework for ensuring the physical protection of nuclear material used for peaceful purposes, including while in international transport. With certain exceptions, the Convention and its Amendment also apply to nuclear material in domestic use, storage and transport.

1.7. Requirements for the safe transport of radioactive material are established in IAEA Safety Standards Series No. SSR-6 (Rev. 1), Regulations for the Safe Transport of Radioactive Material, 2018 Edition [13]. General requirements for radiation safety are established in IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [14].

1.8. Practical information concerning the interface between nuclear safety and nuclear security is provided in Ref. [15].

OBJECTIVE

1.9. The objective of this publication is to provide detailed guidance to States and their competent authorities on how to implement and maintain a nuclear security regime for the transport of nuclear and other radioactive material. This publication may also be useful to operators, shippers or carriers, and others with transport security responsibilities for designing their transport security systems.

1.10. The publication builds upon relevant recommendations in Refs [1, 3] and provides additional explanations of how to implement these recommendations in practice. This publication also complements the guidance provided in Refs [2, 4].

SCOPE

1.11. The primary focus of this publication is the security of nuclear and other radioactive material during transport. It therefore provides guidance on protection against unauthorized removal and sabotage of nuclear and other radioactive material during transport.

1.12. This publication does not cover specific nuclear security measures to locate and assist in the recovery of lost, missing or stolen nuclear and other radioactive material. Detailed guidance on this topic is provided in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [16]. Emergency arrangements pertaining to the response to a nuclear or radiological emergency involving such material are not addressed in this publication; such arrangements are covered in Refs [14, 17–22].

1.13. This publication addresses the interface between nuclear safety and security during the transport of nuclear and other radioactive material, taking into consideration the requirements established in SSR-6 (Rev. 1) [13] and other regulations, standards, codes and guides developed for safety purposes.

1.14. While this publication provides detailed guidance on transport specific measures with respect to the protection of security related information and computer security measures, more general guidance on these topics may also be found in IAEA Nuclear Security Series Nos 23-G, Security of Nuclear Information [23], and 42-G, Computer Security for Nuclear Security [24].

1.15. The guidance presented in this publication is consistent with the Model Regulations [5], and some specific security measures are complementary to those found in the Model Regulations.

STRUCTURE

1.16. Section 2 provides an overview of the categorization of nuclear and other radioactive material from the perspective of nuclear security. Section 3 offers guidance on the responsibilities of the State in establishing a transport security regulatory regime. The focus of Section 4 is the design and evaluation of a nuclear security system for such material in transport. Section 5 addresses the implementation of transport security measures, and Section 6 outlines the process for the preparation, approval and evaluation of a transport security plan. Finally, guidance on maintaining

security during transport, including consideration of safety and security interfaces, is provided in Section 7.

2. CATEGORIZING NUCLEAR AND OTHER RADIOACTIVE MATERIAL AND ASSIGNING TRANSPORT SECURITY LEVELS

2.1. To ensure a graded approach to the security of nuclear and other radioactive material in transport, it is important to apply a categorization system. This section presents the most widely used categorization systems for nuclear and other radioactive material in transport, as well as the primary purpose for which they are intended to be used, the technical basis for their use and the means by which they are applied. An overview of such categorization systems is provided in Table 1. Further explanations for each system are provided in Refs [1, 4, 5, 13, 15, 25].

2.2. References [1, 2] provide recommendations and guidance on specific transport security measures for each category of nuclear material, in line with the nuclear material categorization presented in the Convention on the Physical Protection of Nuclear Material [11]. Specifically, para. 4.5 of Ref. [1] states:

> "This categorization is the basis for a *graded approach* for protection against *unauthorized removal* of *nuclear material* that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity."

TABLE 1. CATEGORIZATION SYSTEMS AND TRANSPORT SECURITY LEVELS

Material categorization and/or transport security level assignment	Purpose	Technical basis	Application in transport
Nuclear material: Category I, II and III nuclear material See Refs [1, 11, 12]	To assign physical protection levels to protect nuclear material against unauthorized removal (see paras 4.2 and 4.4 of Ref. [1])	Potential for the material to be used in a nuclear explosive device based on the element (e.g. uranium, plutonium), radionuclide, quantity, enrichment level for ^{235}U, and irradiation (if applicable)	Direct application
Radioactive material: Basic transport security level and enhanced transport security level; prudent management practices and additional security measures See Ref. [4]	To define transport security levels and to specify security measures that are to be applied for radioactive material in each transport security level	The transport security measures applied should follow a graded approach, which varies in depth and rigour commensurate with the threat and the potential radiological consequences resulting from a criminal or other intentional unauthorized act that involves radioactive material (see appendix I of Ref. [4])	Direct application
Radioactive sources: Category 1, 2, 3, 4 and 5 radioactive sources; D values See Refs [4, 25, 26]	To provide a simple, logical system for ranking radioactive sources in terms of their potential to cause harm to human health (see para. 1.8 of IAEA Safety Standards Series No. RS-G-1.9, Categorization of Radioactive Sources [26])	Although sources with activities exceeding the D values are considered dangerous, it is not considered realistic to implement enhanced security measures for all sources with an activity exceeding the D values. A threshold of 10 times the D values is recommended to specify the enhanced transport security level for radionuclides listed in Ref. [20], which would include Category 1 and 2 sources (see Ref. [25] and appendix I of Ref. [4])	Indirect application (see 'Transport of dangerous goods' below)

TABLE 1. CATEGORIZATION SYSTEMS AND TRANSPORT SECURITY LEVELS (cont.)

Material categorization and/or transport security level assignment	Purpose	Technical basis	Application in transport
Transport safety: A_1 and A_2 values See Refs [13, 27]	The Q system defines the 'quantity' limits, in terms of A_1 and A_2 values, of a radionuclide that is allowed in a Type A package (see para. I.1 of IAEA Safety Standards Series No. SSG-26 (Rev. 1), Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material (2018 Edition) [27])	The Q system considers a series of exposure routes (internal or external) of persons in the vicinity of a Type A package involved in a severe transport accident (see paras I.8 and I.14 of Ref. [27])	Direct application for transport safety regulations Indirect application for security (see 'Transport of dangerous goods' below)
Transport of dangerous goods: All dangerous goods and high consequence dangerous goods and corresponding security provisions See Ref. [5]	To specify the security provisions that must be applied for the conveyance, shipment and/or packaging of radioactive material	The activity threshold for the application of the enhanced security level is 10D for the radionuclides listed in Ref. [25] and $3000A_2$ for all other radioactive materials	Direct application

2.3. The recommendations and guidance in Refs [3, 4] on transport security for radioactive material are consistent with the Model Regulations [5] (i.e. Class 7 radioactive material). The Model Regulations use a threshold to differentiate between high consequence radioactive material packages and other radioactive material packages, proposing requirements for the security of dangerous goods in all modes of transport as follows:

(a) General provisions for the security of dangerous goods, including Class 7 dangerous goods;
(b) Specific security provisions for high consequence dangerous goods, including high consequence radioactive material.

2.4. Paragraphs 3.11 and 3.12 of Ref. [4] state:

> "3.11. States should use one of the following to determine the activity threshold for categorization of radioactive material for transport security:
>
> (a) For radionuclides listed in annex I of Ref. [25], an activity equal to or exceeding that for a Category 2 radioactive source[6] (ten times the D value);
> (b) For all other radionuclides, an activity of $3000A_2$ or greater.
>
> …….
>
> "3.12. A State should also define which radioactive material poses very low potential radiological consequences if subject to unauthorized removal or sabotage and thus does not represent a substantial security concern. Packages containing such material do not need to be assigned a transport security level and only need to be controlled through prudent management practices.
>
> "[6] Radioactive sources with activities between 10D and 1000D are also referred to as Category 2 and greater than 1000D are referred to as Category 1."

2.5. Appendix I of Ref. [4] describes three transport security levels: (a) prudent management practices; (b) basic transport security level; and (c) enhanced transport security level. It also describes the method by which A_2 and D values are used to define the activity threshold for assigning radioactive material to a transport security level. With regard to prudent management practices, para. 3.13 of Ref. [4] states that "no specific security measures beyond the control measures required by the safety regulations and prudent management practices already implemented by shippers and carriers are recommended." With regard to the

basic transport security and enhanced transport security levels, guidance on more stringent security measures is provided in Ref. [4].

2.6. During transport, different materials may be present in the same conveyance[3] or combined on multiple conveyances as part of a convoy. Therefore, the need may arise to assign a transport security level to an aggregation of nuclear or other radioactive material. Detailed guidance on how to calculate the category for an aggregation of nuclear material is provided in paras 4.6–4.17 of Ref. [2] and for an aggregation of other radioactive material in paras 3.26–3.28 of Ref. [4].

3. DEVELOPING AND IMPLEMENTING TRANSPORT SECURITY REGULATIONS

3.1. This section provides guidance for States that are developing or updating their transport security regulations and overseeing the implementation of these regulations in accordance with the national legislative framework for the security of nuclear and other radioactive material in transport. Detailed guidance is also provided in IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security [28].

DEVELOPING REGULATIONS FOR TRANSPORT SECURITY

3.2. The overall goal of developing regulations for the security of nuclear and other radioactive material in transport is to establish a basic set of requirements for the protection of these materials against unauthorized removal and sabotage during transport.

3.3. Clarity in relation to the roles and responsibilities of all of the stakeholders facilitates the understanding and use of regulations by operators and shippers or carriers. During the process of developing regulations, it is good practice to establish a drafting committee to work with the relevant authorities to ensure that all of the transport security laws, requirements, agreements and conventions observed by the State are reflected in the regulations for transport security. This

[3] 'Conveyance' is defined in SSR-6 (Rev. 1) [13] as follows: "(a) For transport by road or rail: any *vehicle*; (b) For transport by water: any *vessel*, or any hold, compartment, or *defined deck area* of a *vessel*; (c) For transport by air: any *aircraft*."

drafting committee could include legal and technical specialists from the relevant competent authorities.

3.4. Regulations should be developed to account for all modes of transport (i.e. road, rail, air and water) permitted in the territory, as well as for domestic and international transport. The chain of custody and responsibility to ensure accountability for a package during transport should be considered during the development of regulations. The required level of security needs to be maintained throughout the duration of the shipment, including during intermodal transfers, interim storage, and in the case of a transfer of custody or a change of responsibility, in terms of security between different operators and shippers or carriers.

3.5. Any operating conditions or equipment used within the State should be identified and considered in the development of the regulations to ensure that the regulations can be applied in a cost effective and practical manner.

3.6. All of the responsible competent authorities, operators and shippers or carriers should have clearly defined roles and responsibilities, outlined in the transport security regulations, in accordance with the functions that they perform and consistent with the type of material and mode of transport used.

Developing a comprehensive understanding of transport within the State

3.7. Before developing transport security regulations, the competent authority should have a comprehensive understanding of the nature and the uses of nuclear and other radioactive material within the State, as well as the threats to such material. This understanding will help the competent authority to identify involved shippers or carriers and receivers in the State, as well as the type of material, and the frequency and mode of transport. In addition, it is advisable to ensure that the transport security regulations can accommodate changes in the use of nuclear and other radioactive material within the country, as well as potential needs for trans-shipments.

Examining national regulations, international agreements and associated administrative measures

3.8. The competent authority should examine national regulations, international agreements and associated administrative measures to identify existing security measures or processes that could be used to support the transport security objectives. For example, if trustworthiness verification is already performed by other competent authorities, the existing process or the information gathered could

be used to verify or accept the trustworthiness of people involved in transport security. Other existing regulations (e.g. related to transport safety, environmental protection or emergency response) should also be taken into account when allocating roles and responsibilities for transport security to ensure a compatible allocation of responsibilities to operators and shippers or carriers.

3.9. The State may already have regulations that cover the identification and protection of sensitive information and that establish levels of information sensitivity, as well as accepted methods for developing, reproducing, granting access to, transmitting, storing and destroying such information. The competent authority may therefore be able to use these regulations and measures when developing transport security plans, security measures, routes, contingency plans, emergency response plans and provisions for the transmission, storage and handling of associated sensitive information (see also paras 6.12–6.14).

Consulting with stakeholders

3.10. When developing the objectives, scope and content of transport security regulations, the competent authority should consult with all relevant stakeholders. Through such consultations, the competent authority can reconcile and resolve potential inconsistencies that might arise involving other regulations; for example, regarding the responsibilities of relevant competent authorities (e.g. those responsible for transport safety, for a specific mode of transport, for the transport of dangerous goods or for the security of facilities that ship or receive nuclear or other radioactive material).

3.11. After the regulations are drafted, the competent authority should, if permitted by national law, provide sufficient opportunities to all relevant stakeholders to comment on the draft regulations and to identify any challenges that they might face in the practical implementation of the regulations. The competent authority may redraft the relevant requirements to address such challenges, to the extent possible.

3.12. During this consultation process, the competent authority should respond to stakeholders' comments to the extent possible, in an open and transparent manner, on the basis of legal requirements in the State. This approach provides an opportunity for the competent authority to clarify prescriptive requirements and/or performance objectives, and thus avoid potential misinterpretations of the regulations. The approach establishes a clear line of communication between the competent authority and stakeholders, which can contribute to the efficient implementation of regulations.

3.13. After promulgation of the regulations by the State, the competent authority should communicate the regulations, their content and the relevant enforcement mechanisms to the public and to operators, taking into consideration national requirements for the protection of sensitive information. Conducting outreach activities with the relevant transport stakeholder groups could facilitate communication among them with regard to these regulations. Guidance could also be developed and communicated by the competent authority to assist operators in complying with regulatory requirements.

Consistency of regulations for the security of nuclear and other radioactive material in transport

3.14. National regulations for transport security that relate to nuclear and other radioactive material should be consistent with relevant international instruments and with IAEA recommendations and guidance, to achieve the following:

(a) Ensure compatibility between transport regulations in shipping, receiving and transit States;
(b) Streamline the preparation of international shipments and the transport approval process through bilateral and multilateral agreements;
(c) Minimize potential security lapses that might result from conflicting or incomplete requirements when international shipments enter or exit the State;
(d) Reduce the risk of loss, diversion or theft of nuclear and other radioactive material during transport that may be related to potential shipment delays and additional in-transit storage time;
(e) Avoid denial or delay of shipments because of problems with ensuring compliance with different requirements;
(f) Ensure an effective interface with the requirements established in SSR-6 (Rev. 1) [13];
(g) Provide transit States with the necessary information on consignments to facilitate transit operations.

REGULATORY OVERSIGHT FOR TRANSPORT SECURITY

3.15. The transport security system used by an operator, shipper or carrier should be subject to oversight by the State's competent authority. Regulatory oversight aims to improve the security of nuclear and other radioactive material during transport and to build stakeholder confidence in the robustness of transport security measures.

3.16. The legislative and regulatory framework should clearly describe the activities to be undertaken by the competent authority as part of its responsibilities for regulatory oversight. The regulatory oversight programme should include basic functions, including authorizations, licensing, inspections and enforcement.

3.17. Legal authority should be granted to the competent authority's personnel, allowing them to conduct inspections for transport security to verify compliance with applicable licence conditions, including compliance with the transport security plan (see also Ref. [2]).

3.18. The basic functions of regulatory oversight enable the competent authority to clearly identify and define the licence conditions and to verify that the activities of the licensee are in compliance with the transport security regulations, with the licence conditions and, where applicable, with the transport security plan. The competent authority can also use a graded approach to issue warnings or monetary penalties, suspend activities or revoke licences as a result of non-compliance with licence conditions on the part of shippers or carriers.

3.19. The competent authority should ensure that the findings resulting from inspections are reviewed to assess the performance of all elements of the transport security system, as well as to investigate non-compliance and determine if any corrective action is needed.

3.20. The purpose of a regulatory oversight programme should also be to verify, prior to any shipment, the compliance of the shipment with transport security regulations, the licence conditions and, where applicable, the transport security plan. In the case of non-compliance, the competent authority should ensure that sufficient corrective actions are taken to allow for the departure of the shipment.

Regulatory inspections

3.21. Depending on their purpose and objectives, inspections may involve examination of the following elements of the transport security system of a licensee:

(a) Security systems put in place at a trans-shipment point for temporary storage, or on conveyances or loads;
(b) Administrative elements, such as information security, personnel security and personnel training and competence;
(c) Transport security plans, contingency plans, response plans, tracking arrangements, communication arrangements, training capabilities and arrangements, guards and response forces;
(d) Security exercises and tests.

3.22. There are three main types of transport security inspections for designated sites, activities and conveyances: (a) announced or routine inspections that have been coordinated with the licensee in advance; (b) unannounced inspections; and (c) reactive, short-notice inspections resulting from information received or because of a security event. These inspections may be conducted in several locations, including at the operator headquarters, storage facilities, conveyance loading areas, temporary or in-transit stops, trans-shipment points and final destinations. The location of the inspection will depend on the purpose and outlined objectives of the inspection. Unannounced transport security inspections should be carefully planned by the competent authority and coordinated with escorts, guards and response forces, as appropriate.

3.23. Inspectors should have appropriate training, thorough knowledge of the relevant regulatory requirements and of the licence conditions, practical knowledge of the security elements to be inspected and knowledge of interfaces with other areas, such as radiation protection, emergency planning and transport safety requirements. For example, for the inspection of arrangements for escorts, guards and response forces, the inspector should have an in-depth understanding of the relevant national requirements and some knowledge of convoys and response forces. For inspections of administrative arrangements relating to an international shipment, the inspector should be familiar with the transport security requirements in the transit States, as well as with any legally binding regional or international requirements. One of the purposes of regulatory oversight and inspections is to assess and ascertain whether licensees have the necessary knowledge and understanding of the relevant topics so that they can ensure the security of transport involving nuclear or other radioactive material.

3.24. Inspections should be conducted using a graded approach, and the purpose of each inspection should be clearly stated. In preparing for an inspection, the inspector should perform a detailed review of the approved transport security plan, if applicable, as well as a review of relevant information from other competent authorities. Other actions to be taken in preparation for an inspection are to estimate the duration of the inspection, notify the people to be involved in the inspection, make administrative arrangements and prepare the equipment to be used during the inspection. An inspection checklist can help to ensure that inspections are both complete and thorough.

3.25. An inspection may begin with an initial meeting between the competent authority and the managers or representatives of the shipper or carrier to explain the purpose and the scope of the inspection. The inspection activities should be conducted according to the approved transport security plan and the relevant

transport security regulations. Findings, facts, assessments and recommendations should be recorded along with supporting evidence by the inspector in the inspection report in a clear and logical manner, with supporting evidence. The report should also identify good practices, non-compliances and significant security issues. Inspection reports should be peer reviewed and shared with any relevant stakeholders for information and decision making purposes, taking into account any need for the protection of sensitive information. Inspection reports should be stored, archived and appropriately protected.

3.26. After an inspection, the inspector should clearly indicate whether any follow-up action should be taken in response to non-compliance issues. Depending on the severity of the issue, a shipper's and/or carrier's licence or authorization to operate may be suspended or terminated. Good practices, along with examples of findings and corrective actions taken to mitigate non-compliance, where appropriate, should be shared with shippers or carriers, as well as with others who may benefit from this knowledge, but only on a need to know basis.

3.27. After the inspection has been conducted, a debrief should take place with the senior managers of the licensee. This debrief could relay details of any non-compliance or other issues identified, the reasons for non-compliance or for other issues, good practices and further actions to be taken. Debriefing activities should also be organized for other inspectors of the competent authority to identify learning opportunities.

3.28. Recordings, findings, assessments and recommendations relating to transport security can be distributed to shippers or carriers to provide direction and to support the enforcement of requested actions.

4. DESIGNING AND EVALUATING TRANSPORT SECURITY SYSTEMS

4.1. Paragraph 4.3 of Ref. [4] states:

> "The regulatory body should select a regulatory approach that the shipper, carrier, receiver and others engaged in transport are required to follow to meet the applicable security goal for a given transport security level. The following are three distinct approaches that the regulatory body may use:
>
> (a) A prescriptive approach, in which the regulatory body specifies the security measures that the shipper, carrier, receiver and others engaged in transport should implement for a given transport security level;
> (b) A performance based approach, in which the regulatory body requires the shipper, carrier, receiver and others engaged in transport to design a nuclear security system and demonstrate to the regulatory body that the system meets a security goal set by the regulatory body;
> (c) A combined approach, in which the regulatory body draws on elements of both the prescriptive and performance based approaches."

4.2. In a prescriptive approach, the transport security system should comply with the administrative and technical requirements specified in national regulations. In a performance based approach, the transport security system should be designed to meet the national security objectives, taking into account the national nuclear security threat assessment, design basis threat and representative threat statements [29]. Many States select a combined approach, with licensees using a mix of the prescriptive and performance based approaches.

4.3. Whether a performance based approach or a combined approach is used for the development of transport security systems, a systematic process is followed, comprising the three phases below (see also Ref. [30] and IAEA Nuclear Security Series No. 40-T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities [31]):

> Phase 1: The operator identifies the specifications for the transport security system in accordance with the national security objectives, requirements and specifications. This phase includes the identification of targets, the assessment of the threat information, the characterization of the conveyance, and the establishment of the operating conditions and the physical and environmental conditions.

Phase 2: The operator designs the transport security system. This phase includes consideration of the conveyance configuration and the design of the security system, such as measures for detection, delay and response.

Phase 3: The operator assesses the effectiveness of the transport security system. This phase includes steps for conducting vulnerability assessments, performance testing and scenario analysis.

4.4. The results of phase 3 will determine whether the design is ready for implementation and whether the existing system is adequate or a new design is needed. If the national security objectives or design specifications defined in phase 1 are not met by the outputs of phase 3, either a new system should be designed or the existing system should be enhanced, with emphasis placed on addressing the weak areas identified in the phase 3 analysis.

4.5. The sequencing of these three phases and a summary of the activities included in each phase are illustrated in Fig. 1, which has been adapted from figure 1 of Ref. [31] for application to transport security systems. A more detailed explanation of the three phases is provided in paras 4.6–4.25.

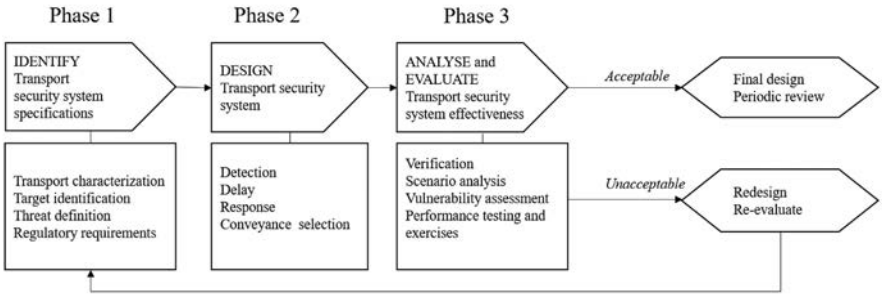

FIG. 1. Process for the design and evaluation of a transport security system (adapted from figure 1 of Ref. [31]).

PHASE 1: IDENTIFYING SPECIFICATIONS FOR THE TRANSPORT SECURITY SYSTEM

4.6. During phase 1 of the process for developing a transport security system, in the context of a performance based or combined approach, the operator should prepare appropriate documentation to identify the security specifications for the conveyance and for other elements of the system (e.g. escort vehicles, communication devices, security personnel equipment, transport control centre layout, equipment). Specifications should also be set out for normal operations and for contingency situations. The term 'normal operations' refers to the routine use of the conveyance, without any particular safety or security concerns. The following factors should be considered in this documentation:

(a) Transport characterization;
(b) Target identification;
(c) Threat definition;
(d) Regulatory requirements and other international or national standards.

4.7. The security specifications should be presented to the competent authority for approval and should be taken into consideration when the operator is drawing up contracts with third parties for the shipment of material or when the operator is procuring security equipment that will be used during transport.

4.8. The operator should evaluate the characteristics of the material being transported and the environment surrounding the shipment, including a review of potential threats and of the robustness of the transport infrastructure. To identify potential threats, the evaluation should integrate information provided by law enforcement agencies, intelligence agencies, relevant security agencies and other relevant competent authorities.

PHASE 2: DESIGNING THE TRANSPORT SECURITY SYSTEM

4.9. During phase 2 of the process, the operator should design the transport security system, taking into account the results of the evaluation conducted in phase 1. The design of the transport security system should include measures to provide detection, delay and response functions (see Section 5 and Ref. [4]).

Selecting the conveyance

4.10. Given the safety hazards and security threats associated with the transport of nuclear and other radioactive material, selecting the conveyance can be difficult. The operational life cycle and the maintenance needs of the conveyance should be taken into account, as well as the operational conditions of the security system, such as the type of road, weather conditions and user needs in relation to the conveyance. The safety system and the security system of a conveyance are closely linked and are often located on a single platform that needs to operate while in motion, making it necessary to consider the interactions between transport safety and transport security elements.

4.11. The operator should also give some consideration to general specifications for the conveyance, including the load handling capacity, the number of personnel needed to operate the conveyance, and the gross weight of the conveyance, as well as its physical dimensions and operational speed.

4.12. The operator should consider the specifications for both normal operations and emergency situations. Emergency situations involve specific safety and security concerns that the conveyance may encounter during operations, such as the planned response to nuclear security events. Examples may include ballistic and explosive protection for the operator or driver, as well as for the cargo and drivetrain. Emergency situations may include a collision of the conveyance with another vehicle, vessel or aircraft, a fire (resulting either from a collision or from another abnormal event) or a breakdown of the conveyance.

4.13. Maintenance specifications should outline how frequently routine maintenance should be performed and which components need to be replaced at what intervals. Preventive maintenance also needs to be performed on a regular basis. Life cycle specifications concerning the expected useful life of the conveyance, from production through decommissioning and disposal, should be considered.

4.14. Specifications for security during storage should also be considered; for example, while the conveyance is not in use, is in temporary storage or is in transit storage. The necessary level of security for the conveyance and/or package should be maintained until the ensuing movement of material.

PHASE 3: ASSESSING THE EFFECTIVENESS OF THE TRANSPORT SECURITY SYSTEM

4.15. During phase 3 of the process for developing the transport security system, the operator should assess the performance of the system. This assessment determines whether the system meets the security objectives with respect to the threat assessment and/or design basis threat for the conveyance. Methods for evaluating the performance of the transport security system are outlined in paras 4.18–4.21. The selection of a specific method will depend on the national regulatory requirements, the technical capabilities of the operator and the resources allocated to complete the analysis.

4.16. For the performance based approach or combined approach, based on an analysis of the effectiveness of the transport security system, transport security experts with specific knowledge of the system's equipment and components should conclude whether or not the system meets the defined performance objectives (e.g. whether the system can delay an adversary long enough for the response forces to arrive). If the system does not meet the objectives and is thus not considered acceptable, it should be upgraded or re-evaluated. An upgrade would involve improvements to existing security measures or the implementation of additional security measures to meet the performance objectives, without having to redesign the entire transport security system.

4.17. The transport security system should be evaluated on a regular basis, even if the initial analysis has determined that the system meets the performance objectives. This ongoing re-evaluation ensures that the system remains effective when threats change, when technology ages or becomes obsolete, or when additional regulatory requirements are imposed.

Use of scenarios to evaluate the effectiveness of the transport security system

4.18. Scenarios can be used to evaluate the effectiveness of the transport security system against a potential threat. Scenarios describe the ways and means by which an adversary might choose to undertake a criminal or other intentional unauthorized act, such as theft or sabotage of nuclear or other radioactive material. Scenarios are hypothetical but should be realistic, credible and consistent with the threat assessment and/or design basis threat. For this reason, qualified experts with a background and experience in law enforcement, security or intelligence, and with an understanding of potential adversary tactics, should be involved in the development of the scenarios used to evaluate the transport security system.

4.19. Key issues that should be considered by experts when developing scenarios include the following:

(a) Adversary characteristics;
(b) Likely location and time of an attack;
(c) Potential use of diversions, deception or surprise;
(d) Use of insiders, both active and passive;
(e) Potential methods to stop the conveyance;
(f) Potential methods to gain access into the cargo compartment;
(g) Number of adversaries needed to breach the cargo compartment;
(h) Use of improvised explosive devices, including those involving vehicles.

4.20. The development of a scenario also involves the creation of a detailed adversary attack plan. Sufficient data should be collected to produce a clear adversary attack plan that appropriately describes adversary actions and includes timelines, coordination steps of the adversary, and a list of assumptions held by the adversary at the time of the attack. The development of an adversary attack plan should include the following four steps:

(1) Identifying the potential vulnerabilities of the convoy, such as those associated with the conveyance, the route and the transport security system, as well as the capabilities of the personnel involved in the transport;
(2) Creating a detailed list of tasks that the adversary has to complete to achieve the projected goal, beginning with initiation of the attack;
(3) Creating a plan to describe how the adversary can accomplish the tasks identified in the previous step, including the time needed for the completion of each task;
(4) Examining multiple attack plans.

4.21. Once the scenarios are fully developed (i.e. with the inclusion of an adversary attack plan) and are made available through the competent authority, they can be used to conduct either a vulnerability assessment or performance testing and exercises, as described in paras 4.22–4.23.

Vulnerability assessment and risk assessment

4.22. A vulnerability assessment can be described as a systematic methodology for analysing the performance of administrative and technical measures against a threat. The results can be used to evaluate the specifications of the transport security system against the national threat assessment or design basis threat. The vulnerability assessment is used by the operator to determine the effectiveness of

security technologies and protection strategies employed in the proposed security system, to define its strengths and weaknesses and to develop cost effective and balanced upgrades. Additional information on vulnerability assessments for the security of nuclear material in transport is provided in paras II.1–II.21 of Ref. [2]. For radioactive material, a security risk assessment should be used as explained in para. 4.35 of Ref. [4].

Limited scope performance testing and exercises

4.23. Limited scope performance testing and exercises are two methods used by the operator to test the transport security system's performance. Limited scope performance testing involves the examination of a specific element of the transport security plan to ensure that the security measures associated with this element function as designed. For example, a communication system or a set of procedures could be tested. It is important to differentiate compliance testing (e.g. whether a sensor reports an alarm) from effectiveness testing (e.g. how well a sensor performs on a sliding scale). Exercises are scenario based performance tests, such as drills, tabletop exercises and field exercises, that use a realistic and credible scenario consistent with the threat assessment and/or design basis threat to evaluate the performance of any aspect of the transport security plan. More detailed information regarding transport security exercises is provided in Ref. [32].

After-action review

4.24. After a shipment has been successfully completed, the licensee should conduct a review to determine if there were any gaps or vulnerabilities during the shipment and, if so, should consider potential improvements that could be implemented in future transport operations. This after-action review is typically associated with, and governed by, the integrated management system or quality management system of the licensee. Competent authorities and licensees — and potentially law enforcement officials — should participate in the review process to identify areas for improvement; for instance, in relation to regulatory oversight, transport security planning processes, the effectiveness of operational security and specific nuclear security response measures.

4.25. The after-action review could include surveys of the organizations involved in the shipment in order to identify lessons and collate good practices for use in future shipments. Debriefs could also be conducted by all relevant organizations immediately after completion of a shipment.

5. IMPLEMENTING TRANSPORT SECURITY MEASURES

5.1. In accordance with paras 5.24–5.30 of Ref. [2] and paras 4.14–4.29 of Ref. [4], the functions of a transport security system are as follows:

(a) Deterrence, which includes features that are visible and are intended to deter criminal or other intentional unauthorized acts, as well as provide protection if such acts are attempted. These features could include visible security measures built into the conveyance and/or the use of guards and convoys. Such measures could also perform other security functions, although they should not affect the safety design of the transport packages.
(b) Detection, which includes activities to provide early detection and assessment of a criminal or other intentional unauthorized act against a shipment of nuclear or other radioactive material.
(c) Delay, which includes activities to prevent access to nuclear or other radioactive material or impede attempts to carry out criminal or other intentional unauthorized acts. In principle, the physical delay time should equal or exceed the time needed for a response force to arrive.
(d) Provision of notification to the appropriate authorities of the following:
    (i) Attempts at criminal or other intentional unauthorized acts, or successful criminal or other intentional unauthorized acts;
    (ii) Responses designed to interrupt criminal or other intentional unauthorized acts;
    (iii) Efforts to assist in the recovery of material stolen during a successful criminal or other intentional unauthorized act.

5.2. The integrated set of transport security measures implemented to fulfil the security functions that are listed above constitute the transport security system. When establishing a transport security system, the interactions between the three security functions should be taken into consideration. Without timely detection, for example, delay measures might be less effective because the adversary will have more time to overcome the protection measures; without sufficient delay measures, the amount of time to provide an effective response might be limited. In addition, the response forces that intervene in a security event are often located at some distance from the nuclear or other radioactive material when the event occurs, thus prolonging the intervention time. Finally, these integrated security measures provide defence in depth to minimize any weak links in the overall security system.

5.3. In a transport security system, security measures can fulfil more than one security function. For example, a lock typically provides a delay function during an attack, but it can also be used to detect attempted theft after the shipment has been concluded. Escort forces can both detect a criminal or other intentional unauthorized act and provide deterrence and response functions.

5.4. Additional security measures may be warranted for certain shipments, depending on the category, type or quantity of nuclear or other radioactive material, the nature of the threat, the capabilities and intent of potential adversaries, and the difficulty and/or sensitivity of a particular shipment, according to criteria determined by the State. A means of dialogue between the competent authorities and operators should be established to communicate on issues related to a potential increase in the threat level, which may necessitate additional security measures beyond those stipulated in the regulatory requirements. Situations that warrant additional security measures might include shipments during a major public event (e.g. a sporting or political event), shipments during political or social unrest, shipments through extremely remote or extremely populated areas, and shipments through areas with poor governmental control.

5.5. Transport security measures may comprise technical measures (e.g. locks, seals, armour, intrusion detection equipment) and administrative measures (e.g. allocation of responsibilities, application of procedures, assignment of the number of personnel) that can be implemented during transport. Paragraphs 5.8–5.71 describe such measures for the conveyance, escort and transport control centre. Paragraphs 5.72–5.88 provide guidance on the communications systems and on the training and qualification of personnel for transport security systems.

5.6. Shippers or carriers can use national and international standards as references for detection equipment, protective equipment and communications devices when designing and implementing their transport security systems.

5.7. Security features presented in this section should not compromise safety in any way and should therefore be analysed, during the design of the transport security system, from the perspective of both the security benefit and any potential reduction in safety.

TRANSPORT SECURITY MEASURES RELATING TO THE CONVEYANCE

Technical measures relating to the security of the conveyance

Tamper indicating devices

5.8. Tamper indicating devices, when applied to conveyances, cargo compartments, packages, freight containers or essential security controls, provide a means of detecting unauthorized access or tampering. Such devices include seals, which can be applied to packages, overpacks and freight containers and constitute an integral part of the approved shipping configuration for the detection of potential unauthorized access to material. The regulatory requirements might dictate which seals the operator can use, or they might prevent the operator from modifying the transport package through the addition of seals or through changes to the type of seal. The selection and application of seals should be integrated into the transport security planning process so as to meet the applicable regulatory requirements. Examples of security seals or high security seals include bolts, cables or electronic seals. All seals should have a unique identification number so as to avoid duplication.

5.9. The practices listed below should be followed when seals are used as tamper indicating devices:

(a) Documentation from the manufacturer should be kept on file, providing proof of the type of seal purchased and the security features of the seal;
(b) An inventory should be maintained of all seals purchased and stored;
(c) Documentation should be prepared for each seal that is affixed, destroyed or removed;
(d) Seals should be issued to, and affixed by, authorized company employees or agents only;
(e) Procedures should be established for reporting any tampered seals that are discovered throughout the supply chain;
(f) Procedures should be established for retaining, or disposing of, used seals that have been removed;
(g) Specific training should be provided to employees, contractors or agents that issue, affix and dispose of seals.

5.10. To assist the designers of transport security systems in selecting appropriate seals whose level of performance befits their purpose, a published international or

national standard[4] should be applied. The standard should address the following three aspects that should be taken into account during selection: (a) testing of the physical strength of the seal (as a barrier to entry); (b) auditing of the security related business practices of the manufacturer; and (c) testing of the seal's capacity to indicate evidence of tampering.

5.11. Mechanical seals should be capable of withstanding harsh environmental conditions, weather and chemicals. They should be resistant to tampering, should be easy to apply and to seal, and should be permanently and uniquely marked and numbered.

5.12. Combined seal and lock devices provide both detection and delay functions for the packages that they secure. The simplest form of such a device consists of a lock with a hole bored through it to allow a passive seal to be attached.

5.13. Passive seals can indicate if a sealed door or package has been tampered with or broken. These seals can be used to ensure that essential communications and operational components are not tampered with. Various types of passive seal (e.g. wired or plastic seals, tamper proof labels) can be used directly on the material container, freight container or truck doors to detect whether they have been opened during transport.

5.14. Electronic seals combine the properties of mechanical seals with an electronic capability to ensure real time notification in the event of the cargo being opened or violated by setting off an alarm. These seals can also store data and provide a communication signal. Such devices might use infrared signals, radio frequency identification (RFID) or other wireless protocols for communication purposes. An electronic seal can be either passive (i.e. a person or device needs to query the system in order to gain information on its status) or active (i.e. information is automatically collected, processed and transmitted to the operator or transport control centre).

5.15. Most types of electronic seal are able to automate seal verification and reporting and to record events such as the opening and closing of doors. In some systems, electronic seals also set off an alarm if they are tampered with or if the seal component is broken. In addition, electronic seal systems are designed to be reusable, which offers an added benefit over mechanical seals. Additional functionalities may include the ability for authentication, delay, location

[4] Any standard used should be established by an independent, non-governmental organization and agreed upon by experts.

tracking, alarm annunciation and automatic data capture. Electronic seals also have drawbacks, however, in that they can be expensive compared with simple mechanical seals, and they may necessitate additional user training and further computer security measures to ensure their integrity owing to their susceptibility to cyber-attacks. Examples of electronic seals include radio frequency enabled door seals, RFID electronic seals, radio frequency enabled package seals and cargo container anti-theft devices with tracking systems.

5.16. For enhanced door or package security, the use of RFID seals that can securely transmit data to an appropriate detection system may also be considered. Such seals can be used to accelerate the confirmation of an intrusion attempt.

Tracking system

5.17. A real time tracking system can use either a terrestrial based positioning system or a satellite based global positioning system (GPS) to monitor the movement of a conveyance. In addition to monitoring the operational state of the conveyance, the tracking system may also be able to determine, using geofencing, if the convoy is moving on schedule along the designated route or if it has left a defined area after having parked.

5.18. Tracking systems are generally available commercially and can be used regardless of the mode of transport. The selected tracking system should incorporate features that secure and authenticate the location information, provide local hardening (i.e. resilience) against cyber-attacks (see Ref. [24]) and operate without any action on the part of the driver. Reports to the transport control centre can be event driven, on demand or scheduled.

5.19. A decision should be made on whether tracking will be used to provide continuous updates on the location of the package and/or conveyance. Considerations important to this decision include the security risks from using a tracking system, such as risk of jamming or spoofing; whether an adversary would be able to monitor the signal; who has access to the data; and the location of the storage of the data, such as in a foreign country.

5.20. Another form of position tracking that might be appropriate for some packages is barcode scanning at each transfer point.

Intrusion detection

5.21. In addition to visual observation, another effective means of intrusion detection is an alarm that alerts personnel to unauthorized access to material being transported by the vehicle. In this case, an audio and/or visual indicator exterior to the conveyance indicates a breach of the cargo compartment. For a visual indicator, a means of visually assessing the alarm is necessary (i.e. through monitors), and a mechanism needs to be in place to send signals to the driver and selected remote personnel (e.g. escorts, response forces and/or personnel from the transport control centre) when attempted intrusion into the vehicle is detected. Mobile duress buttons — installed either in the driver's key or in the crew compartment — and remote communication systems provide means of communicating alarms from an access control or intrusion detection device. Examples of access control and intrusion detection devices include the following:

(a) Balanced magnetic door switches;
(b) Light sensors for closed conveyances;
(c) Passive infrared, microwave or video motion detectors;
(d) Loud, high frequency sirens;
(e) Fibre optic and other electronic seals;
(f) RFID tags that can be affixed to packages;
(g) GPS and cellular tracking of shipments.

Locks, barriers and other delay measures

5.22. All packages should be secured to the cargo bed, generally using strong chains, nuts, bolts, ratcheting and/or related devices. If the material is transported in an open conveyance, the package should also be covered with a heavy duty, waterproof cover (e.g. a tarpaulin) so that the load is not visible or open to the public.

5.23. Passive delay measures include items such as locks, lock shrouds, other locking mechanisms, secure tie-downs, chains, cable nets, reinforced hinges, ballistic glass, armoured plates, tailgate lifts, containers and cages, as well as overpacks and secure tie-downs with locks, cable nets and chains. In addition, passive delay measures include specific operational procedures, such as key control (see para. 5.48). Passive delay measures are most commonly installed in the cargo compartment and on the cargo itself, including on the package.

5.24. Shielded-shackle high security locks can be used for freight container doors and for the container, depending on the configuration. High security locks may prevent or delay attacks by adversaries using handheld tools.

5.25. For most shipments, nuclear and other radioactive material is shipped in standard commercial cargo conveyances or shipping containers. However, inexpensive and easy upgrades can enhance the security of the material; for example, through the use of high strength locks, lock shrouds and heavy duty chains.

5.26. For highly sensitive shipments, special vehicles might be designed or specific transport security system upgrades might be implemented to provide adequate delay measures. For example, the vehicle's load carrying compartment could incorporate panels of multilayer steel armour, thermal insulation, inner and outer steel skins or supplementary barrier materials built on a steel frame. The armour, combined with the overall thickness of the wall panels, provides both access delay and ballistic protection for the cargo.

5.27. The load carrying compartment should be designed to accommodate not only the packages to be shipped, but also the associated transport security system. The decision to armour the load carrying compartment and/or the crew compartment should be based on the load capacity of the chassis. Tie-down tracks used for aircraft cargo could be installed in the cargo floor, side walls and/or roof. The use of cargo tie-down schemes for containers, palletized loads and side wall racks allows more flexibility for loading.

5.28. An access control system that employs two-person controls and/or biometric or multifactor verification can also be installed for the cargo area. An electromechanical locking system could be employed to support such a system.

5.29. When designing a system of delay measures for the cargo compartment, all elements associated with the cargo compartment should be considered from a security perspective to ensure a balanced security system. For example, if a high security lock is installed on the door but the hinges and the door panels are not reinforced, an adversary could potentially force the door without needing to disable the lock.

5.30. If stand-off attacks that involve an adversary creating an explosive release of material are part of a threat assessment or the State's design basis threat, the cargo compartment of the conveyance should be designed to mitigate this type of attack; for example, through multiple physical barriers. In addition to taking advantage of ballistic protection, thermal insulation, overpacks and radiation shielding, other design features could also be employed to counter such attacks.

5.31. The cargo compartment can be constructed using multiple layers of blast resistant material. Compared with having a single thickness of material,

separating multiple layers with other materials and even air gaps has been demonstrated to provide enhanced ballistic and explosive protection. Thermal insulation, which is also a fire retardant, can be used as well to reduce the after-effects of a stand-off explosive attack.

5.32. The package in which the material is transported can also contribute to the security of the material. Packages, such as Type B packages (see SSR-6 (Rev. 1) [13]), are designed to remain intact during transport accidents and can thus provide protection against certain sabotage attempts.

5.33. For transport in a high threat environment, security can be further enhanced by enclosing the package inside a robust protective overpack designed to resist stand-off attacks or unauthorized access. Features of overpacks might include the following:

(a) Package loading and unloading capacity without removal of the overpack from the transport vehicle;
(b) Multilayer wall structure;
(c) Visual decoys, such as non-operational bolts and keys, fixed to the overpack;
(d) Fastening function to lock the overpack to the vehicle from the inside of the overpack;
(e) Foam inner core in the innermost wall for thermal protection;
(f) Double locking mechanical keys to open and close the overpack;
(g) Beacon signal launch function following an unexpected opening of the overpack;
(h) GPS alert and confirmation upon arrival at the destination;
(i) GPS tracking capabilities.

5.34. Cargo restraint systems can also be used to increase the security of the package. For example, restraint systems that are integral to the conveyance structure could be used to secure overpacks or packages to the conveyance, providing improved security by increasing the delay time needed for an adversary to remove the cargo. Additional delay time can be ensured by using restraint fasteners that can be released only by using a special tool. Examples of cargo restraint systems include chain tie-downs with locks and lock shrouds, cable nets and overpacks securely fixed to the cargo bed.

5.35. Conveyances that are specifically designed to resist stand-off attacks and increase the likelihood of guards and transport personnel surviving attacks should be equipped with the following:

(a) Bulletproof tyres that are reinforced with aramid fibre, are shred resistant and puncture resistant, and have steel rims underneath that enable the vehicle to escape at a high speed when the tyres have been destroyed;
(b) Fuel tank protection — for instance, through the application of armour plating, or the use of a specially designed foam tank to prevent the tank from exploding even in the case of a direct hit;
(c) Reinforced steel plates fixed under the vehicle for protection in the case of an explosive being placed underneath the vehicle;
(d) Armour plating to protect the engine;
(e) Grille guards and bull bars made of heavy duty steel, mounted to the front of the conveyance to protect the vehicle occupants in the event of a collision and to allow the conveyance to be driven off road through brush, debris and other obstacles in the case of an ambush.

5.36. Examples of other measures include ballistic barriers (e.g. ballistic windows strong enough to withstand bullets or deflect explosive effects), armour plated doors, anti-carjacking devices (e.g. additional locks on the doors) and discreet driver duress buttons.

5.37. Active delay systems may be used to substantially increase the delay time. They should therefore be considered when designing a transport security system for sensitive shipments from which any loss is considered unacceptable (e.g. shipments of Category I nuclear material) or if the conveyance will be operating at a significant distance from response forces. Active delays can be divided into three broad categories that meet different security objectives: (a) dispenser systems; (b) obscurants; and (c) vehicle operational controls.

5.38. Dispenser systems, when triggered, dispense a material (e.g. sticky foam, tangle wire) that creates a barrier preventing access to the package or material. If unauthorized access is detected, these systems can be triggered manually (by the transport personnel or the transport control centre) or automatically through the actions of the adversary (e.g. when penetration into a defined boundary around the package is detected).

5.39. Obscurants, when triggered and released, create an intolerable or difficult environment that hinders adversaries in completing their tasks. Obscurants can

include smoke, to create a blackout situation, and loud alarms or bright strobe lights, to create a disorienting environment for the adversary.

Vehicle operational control systems

5.40. Vehicle operational control systems can be used as part of the transport security system and are available in two forms: a vehicle authorization system and a vehicle disablement or immobilization system. In both cases, the systems should be protected from physical tampering and cyber-attacks.

5.41. In a vehicle equipped with an ignition sequence security system in which, for instance, the driver performs an authorization process in order to start the vehicle, this may include use of an identification card or device or adherence to a specific order of operations to start the ignition. If identification is confirmed, the alarm system is deactivated and the vehicle can then be started. However, if identification is not confirmed, the vehicle will not start, and a covert or overt alarm will be triggered and transmitted, usually to the transport control centre, signalling unauthorized operation of the vehicle.

5.42. An immobilization or disablement system, when activated, shuts down the vehicle's operating capabilities. Such a system can be activated either from inside the vehicle or remotely, by an escort vehicle or the transport control centre. Immobilization can be reversible; for example, through a variable timer or a manual reset.

5.43. Immobilization features may include the following:

(a) Engine fuel shutoff devices, which disable the fuel pump or the fuel supply system;
(b) Turbo air shutoff valves, which prevent air from entering the engine for combustion;
(c) Accelerator linkage disablement devices, which electronically prevent the acceleration from increasing, with the vehicle's on-board computer control systems slowing the vehicle or preventing acceleration;
(d) Controlled braking systems, which force the vehicle to a stop within a predetermined time after initiation by engaging the vehicle's brakes slowly or at intervals so as to allow the driver to always maintain control;
(e) Brake engagement systems, which cause the brakes to lock, and thus should only be used when the vehicle is stationary, for safety purposes.

Administrative measures relating to the security of the conveyance

5.44. All personnel who are involved with a shipment should hold verifiable documentation, including photographic identification, certificates and operating documents, where applicable, along with any necessary work permits.

5.45. Records associated with the custody and movement of material, such as the chain of custody with transfer signatures, should be maintained. The driver or forwarder should also be provided with the appropriate shipping papers, including a manifest with a schedule and an inventory of the packages.

5.46. The driver and other personnel involved in the shipment should be provided with appropriate operational instructions and training that have the following features:

(a) They are simple to understand and are provided in writing, if necessary;
(b) They explain the roles and responsibilities of the personnel;
(c) They detail the following:
    (i) The security practices to be followed and precautions to be taken to ensure the safety and security of personnel and the cargo;
    (ii) The actions to be taken by personnel before and during the shipment, upon departure and during and following delivery;
    (iii) The actions to be taken by personnel during planned stops (e.g. fuelling breaks, driver relief) and unplanned stops;
    (iv) The actions to be taken by personnel and the responsibilities assigned to them during unexpected events or emergencies.

5.47. The integrity of the security devices attached to packages and conveyances should be verified before departure, prior to recommencing transport after any stop, and after arrival.

5.48. Whenever practical, the introduction of a two person rule is good practice to reduce the insider threat during transport (see IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures Against Insider Threats [33]). For example, the keys to the radioactive material package and the freight container locks could be given to two different persons or, if the conveyance is under escort, one set of keys could be given to the escort team and another set to the driver. Keys to essential locks may be sent to the receiver of the shipment or may travel separately from the shipment. The same approach may be implemented when employing other forms of locking mechanisms, such as key card readers or biometric scanners.

5.49. A vehicle should never be left unattended. A two driver rule ensures that one driver can remain awake, alert and in the vehicle at all times. If, however, there is no option but to leave the vehicle unattended for a short period, it should be locked and immobilized, with the alarm activated (see paras 5.40–5.43). It is good practice to park the vehicle in well lit and secure areas that are under continuous surveillance by security guards or law enforcement officers. When such surveillance is not available, the driver and/or other transport personnel can provide surveillance, in accordance with the regulations and/or the approved transport security plan.

5.50. In the case of a technical breakdown of the vehicle, the carrier should have arrangements in place for repairs in situ or for towing of the vehicle to a repair facility. Carriers should have a plan for moving an inoperable cargo vehicle with nuclear or other radioactive material to the nearest secure location; in this case, compensatory security measures (see paras 6.35–6.38) can be applied until the repair or replacement of the vehicle is complete. If it is not possible to move the vehicle, contingency measures should be in place to create a temporary secured area around the vehicle (e.g. through the deployment of additional escort forces).

5.51. As a precaution against a potential incapacitation of drivers, carriers should also predesignate backup drivers and include them in the convoy. If the convoy stops because of the driver's incapacitation, the escort unit should take measures to ensure the safety and security of the convoy during the exchange of drivers, which could include directing traffic while protecting the convoy.

5.52. A convoy commander should be assigned for each road convoy. The convoy commander has responsibility for relaying information and instructions to and from the crews of each vehicle and is responsible for the safe and secure conduct of the shipment. This person should be the primary contact between the shipment and the transport control centre. The escort commander, who is one of the guards in the escort vehicles, could also be the convoy commander. Deputy commanders could be assigned this function as well.

5.53. The transport security plan should detail the size and structure of the convoy, including the number of conveyances and the number of escort vehicles per conveyance, the spacing between escort vehicles and conveyances, and any limits in terms of the number of vehicles that can be parked at the same stopover site. Owing to the sensitivity of such aggregated information, the transport security plan should be protected for information security purposes, with access authorized on a need to know basis.

5.54. During a shipment, the convoy commander and guards should be responsible for taking all immediate reactive measures. During attempted sabotage, the convoy should make every effort to keep moving, so as to get the cargo to a secure location. If one of the conveyances is disabled, the other conveyances within the convoy may need to continue moving and then park at a safe and secure location to avoid additional exposure to attack. Such movements may involve dividing the escort force and thus should be performed in accordance with the contingency plan. Information should be centralized with the convoy commander and shared with the transport control centre, as well as with law enforcement officials, when appropriate. The necessity of route changes should be assessed alongside law enforcement officials, as per the contingency plan, and should be communicated to the transport control centre.

TRANSPORT SECURITY MEASURES RELATING TO THE ESCORT OF SHIPMENTS

5.55. Armed and unarmed escort personnel should be specially trained and equipped to protect the shipment. These personnel travel either in the transport conveyance or in accompanying vehicles. Both the personnel and the vehicles should be appropriately equipped to communicate with the transport control centre and/or with external response organizations.

5.56. The designers of transport security systems should determine the level to which the guards should be protected and armed, on the basis of the threat assessment or the design basis threat and the potential radiological consequences in the case of sabotage of the material. The designers should also determine the tactics that the guards are expected to use, as well as the use of force allowed by the State. If national regulations require that armed guards be used for a shipment, those guards should be equipped with weapons in accordance with the State's legal requirements and should be provided with personal protective and communications equipment. If the guards are to be armed, the next consideration is the selection of weapons. Examples of possible weapons to be used, in accordance with national law, include side arms (i.e. handguns), long guns (i.e. rifles), automatic and semi-automatic weapons, hand grenades, batons, tasers, pepper spray or other chemical irritants, smoke grenades and flash bangs (i.e. stun grenades). Guidance and procedures should be developed, and training provided, on the conditions in which guards are permitted to employ their weapons, again in accordance with national laws.

5.57. In addition to weapons, guards should be provided with personal ballistic protection, such as bullet resistant vests, ballistic helmets, eye and ear protection, handheld communication devices and other tactical equipment to enhance their response capability, such as tactical ammunition vests.

5.58. Consideration should be given to protecting not only the material, but also the personnel, of both the transport conveyance and the guard force (also referred to as the internal response force) to increase their likelihood of survival in an attack. If a shipment is attacked, the guards and transport personnel can not only provide detection, but also, if properly equipped, delay the adversaries in accomplishing their task. The guards and transport personnel should be able to communicate a duress signal through a mobile or fixed duress button. In an attack, the objectives should be to keep the conveyance moving and to activate other security measures while actively participating in the protection of the shipment.

5.59. If a large number of guards accompanying a conveyance survive the initial stages of an attack, the need for further delay measures is reduced, since these remaining guards can provide delay. Conversely, if this number is small (either as a result of high casualties or because of the small initial number of guards), a greatly increased delay time is needed to allow the remaining guards sufficient time to redeploy in order to defend the cargo. If the shipment is travelling in remote areas, where sizeable secondary response forces are not immediately available, guards play a valuable role in protecting the nuclear or other radioactive material. Their survival is therefore of the utmost importance. In addition, the transport personnel should be able to maintain control of the conveyance and prevent an adversary from using the conveyance to escape with the material.

5.60. Increasing the likelihood that guards and transport personnel will survive in the case of an attack should be considered at the design stage of the transport security system. Building in the necessary protection in the vehicle helps to enhance their chance of survival, but also typically adds considerable weight to the chassis. The gross weight of the chassis, both empty and with the largest expected load to be transported, should therefore be considered. An appropriately sized chassis is essential to ensure that the vehicle functions as designed.

5.61. Accompanying guards should continuously monitor the vehicle and its surroundings. Transport personnel, guards or escorts will likely be the first to assess and validate an alarm that is triggered by the conveyance. A lead reconnaissance vehicle can travel in advance of the shipment to visually assess route situations, raise alarms as needed, potentially redirect the shipment and initiate response force actions as needed.

5.62. For shipments by rail, escorts and/or guards should accompany the shipment to monitor the rail freight car or freight containers carrying the nuclear or other radioactive material. They could travel in an adjoining guard car and use closed circuit cameras to perform monitoring.

TRANSPORT SECURITY MEASURES RELATING TO THE TRANSPORT CONTROL CENTRE

5.63. The transport control centre — whether for transport by road, rail, air or water — is an integral element of the transport security system, serving as a communication and tracking hub. Use of a transport control centre is recommended as an additional security measure for the transport of Category I and II nuclear material. For the transport of Category 1 radioactive sources, the regulatory body might also consider requiring a transport control centre. If a transport control centre is not used as part of the protection strategy, every shipment should nonetheless have a single point of contact for the transport and escort personnel to allow them to call for assistance if necessary.

Technical measures relating to the transport control centre

5.64. The transport control centre should be protected against any threat aimed at influencing or neutralizing its role. In accordance with national strategies, both physical protection systems and computer security programmes and measures (see Ref. [24]) should be in place to protect the transport control centre from the defined threats, as outlined in the threat assessment or design basis threat. Physical and cyber access to the transport control centre should be limited to authorized and vetted personnel. The two person rule should be applied, and measures to prevent unauthorized access should be established and maintained using intrusion detection systems. The transport control centre should also use redundant, diverse and secure communication channels and should be equipped with emergency electrical power.

5.65. The transport control centre should have the ability to continuously monitor shipments, both under normal operations and in emergencies. Monitoring can be facilitated by the transport personnel through reporting at regular intervals. However, the transport control centre should also be tracking the shipment of the material, including the current position and security status, to be in a position to alert response forces in case of an attack. The centre should also maintain continuous and secure two way voice communication and text exchanges with the transport personnel in charge of the shipment and with the response forces.

5.66. The State's competent authority may have its own transport control centre. In this case, the State should make the necessary arrangements for the exchange of information and digital assets among the State's transport control centre, the operator's transport control centre and the transport personnel responsible for the shipment. Regardless of who is operating the transport control centre, consideration should be given to the appropriate level of staffing, operating hours and staff training to ensure proper and effective staffing at all times during shipments.

5.67. For maritime transport, the transport control centre should be located in the flag State of the ship (i.e. the State under whose registration the vessel operates) and should be staffed at all times during shipments by properly trained and vetted personnel. The ship should be equipped with a system that enables the transport control centre to monitor its location at regular intervals and upon request.

Administrative measures relating to the transport control centre

5.68. A formal transport control centre consists primarily of a central point of contact that ensures the continuous monitoring of shipments. The personnel that operate the transport control centre should be in possession of all the necessary information pertaining to the transport, including the material being shipped; the different shipping actors (e.g. shipper, carrier, receiver, freight forwarders); any in-transit points and organizations (e.g. ports, airfields); and information regarding the initiation of response and contingency plans.

5.69. The transport control centre should have information on whom to contact and when, as well as a list of essential information to be conveyed if a nuclear security event occurs during shipment. Such procedures should be formalized in the response and contingency plans.

5.70. While the shipment is in progress, transport control centre personnel should be able to advise the vehicle driver of any incidents, such as a demonstration, road closure or severe accident along the scheduled route, that might have security implications.

5.71. The transport control centre should have priority contact with the convoy commander and other parties involved in the shipment. A clear chain of command should be established, with the correct contact information for all members of the chain. Information on both the chain of command and the communication arrangements should be provided to the transport control centre, the driver of the shipment, the convoy commander and deputy commanders.

COMMUNICATION IN TRANSPORT SECURITY SYSTEMS

5.72. Having two way communication systems in place throughout the shipment is essential, with the two primary types of communication being administrative and operational.

5.73. Administrative communication covers exchanges that occur during the planning and completion phases, including the submission of transport documents (e.g. the transport security plan for regulatory review and approval). It also includes the exchange of pre- and post-shipment notifications among the shipper, receiver, other third party entities (e.g. customs authorities, carriers, operators) and the competent authority. All stakeholders should ensure that this information is transmitted and managed in such a way as to limit distribution to a minimum, need to know basis.

5.74. Operational communication covers all exchanges (i.e. data and voice) that take place during transport, from intra-shipment communication to communication among the personnel responsible for the shipment, its escorts and the transport control centre. A subset of operational communication deals with exchanges during a security event, and more specifically between the personnel responsible for the shipment and external response forces. Since this form of communication is typically undertaken via mobile phone, and thus can be intercepted, those using such communication tools should guard against transmitting any sensitive information. If possible, the transport security organization (e.g. the transport control centre, internal response force, security guards) and the external response forces should share a secure two way communication channel.

5.75. Several operational considerations should be taken into account when planning and developing the communication structure. The most important consideration is that the communication system should function throughout the duration of the shipment. Communication could take place via different platforms (e.g. mobile phone, radio, satellite phone), using different means (e.g. voice, data). Some examples of communication technologies include secure, encrypted handheld communicators, satellite based communications equipment, and mobile or handheld general frequency receivers and transceivers, including those that are of very high frequency and of ultra-high frequency. These communication systems should be encrypted to prevent the general public and adversaries from monitoring communication within the transport system. If open communication is the only option, techniques such as code words and phrases should be considered to provide some protection in communicating sensitive information.

5.76. Other considerations in planning communication include the possibility of employing systems that are interoperable between the networks being used by the transport personnel, the guards and any potential external response forces. The communication systems should also be robust enough to handle various operating environments.

5.77. Provision for communication capability is important for the timely reporting of any security event so as to initiate a response, as appropriate. Therefore, a means of communication (e.g. mobile phone, two way radio, computer, radio, satellite phone with voice and text messaging) should be provided to the drivers, escorts and other transport personnel. Additional means of communication may be considered if the transport is undertaken in remote areas, where a lack of infrastructure necessitates the use of multiple technologies. Having a supplementary means of communication will also help to ensure communication capabilities if one device fails. The standard communication systems, GPS signal, duress buttons and corresponding alarms should all be tested prior to departure of the shipment from the shipping facility.

5.78. Special verbal duress codes should be established prior to each shipment and should be kept confidential. Special passwords can also be pre-established for carriers to verify that they are speaking only to the assigned drivers.

5.79. Drivers and other transport personnel should be given written instructions to be used in the case of a security related event. These instructions should include the location of authorized stops, information on the operation of alarm systems, the actions to be taken in case of theft or sabotage of the vehicle or package, and the telephone numbers of key personnel working for the operator and for law enforcement agencies.

TRAINING AND QUALIFICATION OF TRANSPORT SECURITY PERSONNEL

5.80. Security awareness training is prescribed in dangerous goods transport safety regulations, such as the Model Regulations [5] and those issued by the International Maritime Organization [6] and the International Civil Aviation Organization [7]. Most regional agreements also refer to these international regulations. The training provided on the transport of dangerous goods may also apply to the transport of nuclear and other radioactive material, since these materials belong to Class 7 dangerous goods. Security awareness training could be integrated into existing mandatory safety training, and delivered through

various means, such as on-line, using web based tools or in person training. Any specific security concerns relating to the potential radiological consequences that could result from the nuclear and/or radioactive nature of material should be emphasized during training.

5.81. All persons engaged in the transport of dangerous goods should have basic security awareness training, which comprises an understanding of the need for transport security, the nature of security related threats, methods to address security concerns and actions to be undertaken in the case of a security event. This training should also include information on transport security plans and, if appropriate, on contingency and response plans, commensurate with the responsibilities of individuals and their roles in implementing these plans.

5.82. Security awareness training should be verified upon recruitment or provided by the employer to all personnel involved in the transport of nuclear and other radioactive material. The training should be periodically supplemented by refresher training at intervals determined by the competent authority or the employer.

5.83. Records concerning the security awareness training undertaken by personnel should be maintained by the employer and should be made available to both the employee and the regulatory body upon request. In particular, employers should keep records of the provision of training and/or verification that such training has been received elsewhere and is current, as well as records of any refresher training taken. These records should be kept by the employer for the period specified by the competent authority.

5.84. The State should establish clear criteria for the training of guards or security forces assigned to escort shipments. These criteria should result in the establishment of a training and qualification plan, typically by the shipper or carrier, or by the organization conducting the security escort under contract with the shipper or carrier.

5.85. The shipper, carrier or organization responsible for the security of the nuclear or other radioactive material in transport should not permit any individual to perform duties and have responsibilities related to the security of the material unless that individual has been trained, equipped and qualified to do so in accordance with the training and qualification plan.

5.86. Non-security personnel might also be assigned duties and responsibilities relating to the security of nuclear or other radioactive material. In this case, the personnel should satisfy the following conditions:

(a) Be trained, qualified and periodically requalified to perform their assigned duties through established training programmes;
(b) Be provided with the necessary equipment to perform their assigned duties;
(c) Possess the knowledge, skills and abilities, including physical attributes (e.g. adequate sight and hearing), needed to perform their assigned duties and responsibilities.

5.87. As part of defensive tactics, training and qualification in the selected weapons systems and in personal ballistic protection should be provided to the accompanying guards and response force personnel, along with training on how to employ these systems. The physical fitness of guards should also be a consideration, as well as the ability of guards to make tactical decisions and function as a cohesive element. Guards and responders should receive sustainment training in the above areas, which might include drills, limited scope performance tests and exercises to ensure that they can accomplish their assigned missions.

5.88. Training should also address radiation safety and protection, security threats and risks related to the material being transported, the types of package and the level of radioactivity permitted in each package, as well as response plans and communication.

6. PREPARING, APPROVING AND EVALUATING THE TRANSPORT SECURITY PLAN

6.1. The competent authority should request that a transport security plan be prepared for Category I and II nuclear material as recommended in Ref. [2] and for radioactive material assigned to the enhanced transport security level as recommended in Ref. [4]. A transport security plan may be deemed necessary by the competent authority for nuclear material of Category III and below and for other radioactive material on the basis of the level of threat, the relative attractiveness of the material or other indirect, real or perceived impacts of a security event on the public and society.

6.2. The process of preparing, approving and evaluating a transport security plan is described in this section, which includes examples of good practices. This section also provides guidance on the content of a transport security plan and how to effectively implement and maintain the plan as part of the transport security system.

PREPARATION OF A TRANSPORT SECURITY PLAN

6.3. The competent authority should provide the shipper or carrier with clear descriptions of the content and structure of the transport security plan, along with clearly defined requirements and guidance on its proper preparation and implementation. Following the completion of a vulnerability assessment and the design of a transport security system, as described in Section 4, the shipper or carrier should develop a transport security plan that incorporates a range of security measures, on the basis of the information provided by the competent authority. Appendix I of Ref. [2] presents a sample transport security plan for nuclear material, and appendix II of Ref. [4] presents a sample transport security plan for other radioactive material. A given transport security plan may address a single shipment or multiple similar shipments and may be valid for a defined period or for a specific number of shipments.

6.4. If the shipper or carrier uses a subcontracted carrier or freight forwarder, the shipper or carrier should ensure that this subcontractor meets the criteria of the transport security plan, implements a mechanism to verify transport security measures and retains records. Additionally, subcontractors and their employees who are involved in the transport of nuclear or other radioactive material should undergo the same trustworthiness screening process as that undergone by new employees when recruited by the operator. The responsibility for implementing this process should rest with the subcontractor. The operator should nonetheless request that the subcontractor demonstrate, through its records, that the relevant verifications have been implemented.

6.5. If the shipper or carrier maintains the same transport security plan across multiple shipments, the shipper or carrier should, in accordance with the applicable regulatory requirements, regularly review the transport security plan and update the plan as needed. The transport security plan should also be updated if any significant changes are made to the transport security system, if the threat changes, if processes described in the plan change or if regulatory changes mandate an update. The competent authority may request that the shipper or carrier resubmit the plan at defined intervals for review, and approval if necessary.

6.6. The seven steps outlined below may be followed in the preparation of a transport security plan:

(1) The shipper or carrier designates an individual with overall responsibility for the transport security plan. This person could either be tasked with oversight of a drafting team or be given the responsibility to draft and complete the transport security plan.
(2) A team of individuals is selected according to the responsibilities outlined in the plan. For example, the team might include a radiation protection officer, a security specialist and a logistics specialist. The size of the team should be as large as needed to adequately address security requirements, but it may also be as small as one person.
(3) The outline of the transport security plan's structure is planned and prepared. Considerations for developing a transport security plan are outlined in paras 6.7–6.30 of this publication, and also in appendix II of Ref. [4] and in appendix I of Ref. [2].
(4) Relevant data and information pertaining to shipments are gathered by the responsible individual and/or drafting team and used to develop a draft transport security plan.
(5) The draft transport security plan is approved by the management of the shipper or carrier.
(6) The approved transport security plan is submitted for approval to the competent authority, if required.
(7) If approval is required, the competent authority approves the transport security plan or requests additional information from the shipper or carrier. In the latter case, steps 4–6 are repeated.

Considerations for developing a transport security plan

6.7. In implementing the above steps for the preparation of a transport security plan, the shipper or carrier should obtain input from all relevant stakeholders (e.g. response forces, other competent authorities). This input may include route information (e.g. primary and alternate routes, bridges and tunnels, planned events along the route, road conditions), material and vehicle descriptions, details of the transport convoy composition, and information about escorts (e.g. whether they are armed or unarmed), communication arrangements and delay measures (e.g. vehicle immobilization devices).

6.8. Taken separately, information on the quantity of material to be shipped, the date of the shipment and the route of the shipment might not be considered sensitive, but

when this information is combined with other information, the resulting document should be considered sensitive and should thus be adequately protected.

6.9. Paragraphs 6.10–6.30 provide detailed guidance on other types of information that should be considered for inclusion in the transport security plan.

Threat and vulnerability assessments

6.10. A transport security plan should address the relevant threats contained in the national threat assessment. A threat assessment should be conducted by the State in advance of any shipment. If the threat level is assessed as being high, the shipper or carrier should consider additional security measures or could consider adjusting the routes, itinerary and timing of shipments in order to mitigate risk. More guidance on threat assessments is provided in IAEA Nuclear Security Series No. 10-G (Rev. 1), National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements [29].

6.11. The security system for a transport operation should be assessed to determine if there are unacceptable vulnerabilities in relation to the shipment. This is typically performed through a vulnerability assessment process, during which the transport security plan itself is reviewed and tested (see para. 4.22). The method used to perform the vulnerability assessment should be included in the transport security plan.

Protection of sensitive information

6.12. A transport security plan will inevitably contain sensitive information, such as schedules, routes, security measures and response capabilities, and it should therefore be appropriately protected, in accordance with the national requirements for information security. The transport security plan should be distributed on a need to know basis and strictly to individuals who have been granted a valid trustworthiness verification level, acquired through a background investigation process.

6.13. For information security purposes, the transport security plan as a whole should be protected to the level of the most sensitive information contained within it. The transport security plan may be divided into more than one document or into separate sections that are developed for the purpose of transmitting information on a need to know basis. Such a practice can ensure that those persons with responsibilities under the transport security plan have access only to the information that is necessary for the performance of their duties. For example,

vulnerability assessments are generally considered to contain information that needs a high level of protection and thus should have well controlled, limited distribution. A shipper may choose, or be obliged by the competent authority, to keep the vulnerability assessment separate from the rest of the transport security plan in order to protect the sensitive information contained in the assessment when distributing other, less sensitive sections of the transport security plan.

6.14. Submission of the transport security plan and any accompanying documents to the competent authority, in accordance with the information security controls required by the regulatory body, should be carried out via encrypted email, fax, secure courier or hand delivery (see Ref. [23] for more information).

Planned and alternative routes

6.15. When selecting planned or alternative routes for the transport of nuclear or other radioactive material, the shipper or carrier should consider applicable regulations and ordinances on transport routes for dangerous goods, and in particular any regulatory restrictions placed upon the type of material being transported.

6.16. A State may have more than one competent authority that has responsibility for the movement of nuclear or other radioactive material. For example, a State's highway, rail or general transport authority may impose restrictions regarding the size and/or weight of vehicles permitted to use certain highways and railways. Other authorities in a State may restrict road movement in the vicinity of large metropolitan centres or essential infrastructure, such as nearby dams. Therefore, when planning a route involving intermodal transport, the shipper or carrier should take into consideration the regulations and requirements for all modes of transport used during the shipment.

6.17. The shipper or carrier may also make route selections based on safety and security considerations, for example, road conditions, response times along the route, communication capabilities and speed limits, as well as potential hazards, such as rockslides, floods, snowstorms or forest fires that could adversely affect the shipment. Additional factors to consider, where practical, include avoiding heavily populated or urban areas, selecting routes where response forces can respond effectively and minimizing passage through constrictive infrastructure, such as bridges and tunnels. The shipper or carrier drafting the transport security plan should avoid potential hazards if possible; if this is not possible, the shipper or carrier should have plans in place to deal with any related complications that may arise. For example, if the shipment has to transit through an urban area, the transport security plan may include a description of the precise route to be taken

and how the shipment could be scheduled to avoid times of peak traffic. If transfer points, temporary storage areas, stopover facilities, safe havens or subsistence locations are included in the planned or alternative routes, the transport security plan may make reference to other security plans for these locations.

6.18. Route and scheduling variability are other means of providing significant protection; for example, by not using the same route or not shipping at the same time of day for each shipment. Variability can increase unpredictability for similar shipments (e.g. transport of the same type of nuclear or other radioactive material, use of the same conveyance, use of the same origin and destination), providing considerable protection for shipments. Changing shipping patterns, such as the routes or the timing of shipments, can thus make it more difficult for an adversary to plan and initiate an attack.

6.19. As the first step in the planning of a route, online mapping applications, satellite imagery and aerial photography can be used, bearing in mind that these sources offer only a limited amount of information on the conditions of a chosen route. The shipper or carrier planning the route should consult with relevant authorities to request accurate information on possible routes or conduct their own reconnaissance of planned and alternative routes. Aspects of interest during route reconnaissance exercises might be the conditions of roads, the presence of railways and crossings, tunnels or bridges, the road width, the gradient of the road, ongoing or expected repairs or construction work, and the locations, conditions and supply of refuelling stations. Also important to planning is the physical construction and engineering suitability of the roads to the weight of the conveyance.

Description of the conveyance

6.20. The transport security plan should provide a description of the conveyance, as applicable from the time that the shipment leaves its originating location until it reaches its planned destination. The description should include how the nuclear or other radioactive material will be contained and how it will be secured for transport, the type, design, size and weight of any containers that will be used, and any provisions needed for securing the containers to the conveyance.

6.21. The proposed shipment might involve intermodal transport and/or intermodal transfers. For example, the nuclear or other radioactive material might be transported by road to a rail terminal, loaded onto a railcar and then transported by rail to an airport, where it is then loaded onto a plane, transported by air to another airport, loaded onto a truck and finally transported again by road to the

planned destination site. In this case, the details of each conveyance should be provided separately in the transport security plan, along with the date, time and location of the planned transfers, any planned temporary storage throughout the duration of the shipment and the names of the convoy commanders for each mode of transport.

Proposed security measures

6.22. A description of the proposed security measures to be used during transport should also be included in the transport security plan. To ensure adequate protection during transport, the proposed security measures should be commensurate with the specific circumstances of the transport. For example, these measures should consider the category of material to be transported, the size and type of the consignment, the distance and type of terrain to be covered, the mode of transport, the results of the threat assessment and any public concerns.

Communication arrangements

6.23. A description of the communication arrangements that will be in place throughout the shipment should be included in the transport security plan. This description should cover the types (e.g. mobile phone, radio, satellite phone), methods (e.g. voice, data) and protocols for communication under different operational situations (e.g. normal operations, abnormal events, emergency situations), response and contingency plans for situations in which no communication is possible and redundancy plans for these systems. It should also cover the encryption method(s) used for communication and the degree of security applied to such communication.

6.24. In addition, the communication arrangements to be used within and among units or organizations involved in the shipment (e.g. the shipper or carrier, receiver, response forces, transport control centre) should be described in the transport security plan and should include information on the specific communication methods to be used.

Arrangements with response forces

6.25. The transport security plan should also include descriptions of any arrangements made between the shipper or carrier and the response forces escorting the shipment and/or located along the transport route, taking into account the different jurisdictions and agencies that have response responsibilities along the route of the shipment. The arrangements should include provisions for

establishing effective communication with the various response forces along a transport route. Any changes in the proposed communication methods or communication protocols (e.g. changes in radio frequencies or in radio or mobile encryption methods) should be clearly outlined in the transport security plan. The methods of communication with various agencies, and the jurisdictional and operational boundaries along the route, should be confirmed to be accurate by the shipper or carrier.

6.26. In addition to the communication arrangements, any special security arrangements to be made with the response forces — for instance, those required by the regulatory body for a given shipment — should also be set out in the transport security plan. For example, information on the provision of an armed escort by law enforcement or private security agencies should be included in the transport security plan. Where special security arrangements involve more than one response force, such as movement from one jurisdiction to another or across an international border, the plan should describe the cooperative arrangements for transferring responsibility from one response force to another. The plan should also describe any coordination arrangements between members of the response force and personnel who are involved in the logistical aspects of the shipment (e.g. the driver, escorts).

Contingency planning

6.27. The shipper or carrier should have response and contingency plans in place for responding to different postulated scenarios, including those of low probability, or abnormal events that might impact the security of a shipment. The number and types of scenarios to be covered may be determined by the competent authority or by the operator.

6.28. Situations that might arise during transport and can be addressed via response and contingency plans, include the following:

(a) Technical breakdown of the conveyance or escort vehicles;
(b) Incapacitation of the driver or other convoy personnel;
(c) Delays or stops of the convoy;
(d) Route changes;
(e) Route deviation;
(f) Malfunction of tracking systems, communications or other equipment, suspected GPS jamming or spoofing if satellite navigation is used;
(g) Traffic accidents;

(h) Natural disasters;
(i) Attacks on the shipment, such as attempted sabotage (e.g. disablement of cargo vehicle) or unauthorized removal of material.

6.29. A pre-established route, including possible route changes and deviations, should be agreed by the carrier, law enforcement authorities and competent authorities. In this way, preclearance can be given for unexpected activities that could be taking place along the route (e.g. construction, road maintenance, special events).

6.30. Route changes are typically made as a result of receiving new information indicating that a threat is imminent. In such cases, the convoy should proceed to an alternative, pre-approved route. Route deviations, on the other hand, are typically made because of unforeseen barriers that are not directly threat related (e.g. a fallen tree or traffic accident blocking the road), where passage might be impossible or unrealistic for an extended period. In such cases, the convoy should take an immediate detour to bypass the barrier and then return to its prescribed route as soon as practical. Any intention to take immediate detours should be reported to the transport control centre and conveyance security should be on heightened alert.

APPROVAL OF THE TRANSPORT SECURITY PLAN BY THE COMPETENT AUTHORITY

6.31. If the competent authority requires that the transport security plan be approved prior to the commencement of a shipment, it may choose to integrate this requirement into the licensing and authorization process for the transport of nuclear and other radioactive material. If such a regulatory requirement is in force, it should be communicated to the shipper or carrier to facilitate timely submission of the transport security plan and to allow the competent authority sufficient time to conduct a technical assessment of the plan for completeness and adequacy before approval.

6.32. The competent authority's review of the transport security plan should be based on national requirements for the security of nuclear or other radioactive material in transport (e.g. existing national regulations), the design basis threat or any representative threat statement, the vulnerability assessment, if applicable, and other regulatory documents. For the approval of the transport security plan, the competent authority may request input from relevant stakeholders.

EVALUATION OF THE TRANSPORT SECURITY PLAN

6.33. It is good practice to evaluate the transport security plan or elements that are listed in the plan before a shipment so as to determine its effectiveness. For example, the transport security plan can be evaluated through facilitated discussion, tabletop exercises, drills, or limited or full scope exercises. Reference [32] provides information on the preparation, conduct and evaluation of exercises for the security of nuclear and other radioactive material in transport. These exercises may involve a range of stakeholders, such as law enforcement officials, escort personnel or other competent authorities who have responsibilities related to the transport security plan. Following the evaluation, it is also good practice to capture the identified lessons in an after-action report and to adjust the transport security plan as needed. The validity of the transport security plan should also be evaluated in light of new or changing threat environments or transport conditions. Any resulting adjustments to the transport security plan should be submitted to the regulatory body for approval as necessary.

6.34. Another good practice is to evaluate events or deviations from the transport security plan that occurred during previous shipments and to identify any improvements that need to be made to the transport security plan as a result. The transport security plan should then be updated for future shipments, in particular those of a similar nature (e.g. involving the same type of nuclear or other radioactive material, the same conveyance, or the same origin and destination). The transport security plan is specific to one shipment and should not be used for other shipments without prior evaluation to assess its validity and appropriateness to the specific shipment.

Compensatory measures

6.35. In some situations, it may not be possible to implement the security measures in the transport security plan. Previously approved security measures may also malfunction during transport and the replacement of such measures may not be feasible or reasonable. In such cases, compensatory security measures should be implemented to provide a commensurate level of security.

6.36. Before implementing compensatory security measures, the shipper or carrier should conduct an analysis to determine whether the measures will provide a level of security that is commensurate with that provided by the security measures described in the transport security plan. This analysis should be documented. The proposed compensatory measures should then be submitted to the competent authority, which should approve the measures only if it is satisfied that they

provide a commensurate level of protection. Otherwise, improvements to the compensatory measures should be requested. The considerations described above in relation to information security and the transport security plan should also be regarded as valid here.

6.37. Compensatory measures should be implemented before the commencement of the shipment to ensure that capabilities are in place to detect, assess, interdict and neutralize threats to the shipment at all times and that these capabilities meet the national requirements.

6.38. Examples of compensatory measures include the following:

(a) A security escort to provide a balanced system if the use of multiple physical barriers is not possible during transport.
(b) An intrusion detection system attached to a conveyance or container, or additional delay measures inside the conveyance, such as chains, lock bars or other delay devices, if the use of multiple physical barriers is not possible during transport.
(c) A backup means of communication and an alternative means of determining the location of the consignment if the duress button malfunctions, if a problem arises when trying to transmit or receive information using the GPS signal or if the transport control centre cannot be reached directly.
(d) Requests to escorts to compensate for a lack of communication by the shipment vehicle (e.g. if a key component of the communication system has malfunctioned) by communicating the status of the shipment vehicle to the transport control centre.

7. MAINTAINING SECURITY DURING TRANSPORT

7.1. The continuity of security during different transport operations and events should be an important consideration for States, shippers or carriers, and receivers. These operations and events may include the following:

(a) When a conveyance moves from one State into another;
(b) When a consignment is transferred from one carrier to another;
(c) When an intermodal transfer is undertaken;
(d) When a shipment is stored temporarily until it is accepted by another carrier and/or State;

(e) When unplanned stops occur;
(f) When the personnel involved in the transport change;
(g) When security related information is exchanged between States by electronic media or post;
(h) When an incident or accident occurs during transport that might compromise security arrangements.

7.2. Security measures for which continuity should be assured during transport include the following:

(a) Security measures applied to the conveyance and at the intermodal transfer site, the temporary storage facility or other locations used during transfer from one carrier to another;
(b) Communications during transport;
(c) Tracking devices and their transmission of information by a mobile communications network or satellite based systems.

7.3. Provisions on specific modes of transport and on the continuity of security during transport are provided in Ref. [2] in relation to nuclear material, but they may also be applicable to other radioactive material.

ADHERENCE TO INTERNATIONAL LEGAL INSTRUMENTS AND RECOMMENDATIONS FOR TRANSPORT SECURITY

7.4. While each State is responsible for the security of nuclear material located in its territory, international legal instruments offer a standard framework for States to follow in relation to transport security. More specifically, these instruments manage the continuity of security across borders, between States and in the case of intermodal transfers.

7.5. Several international organizations address transport security for dangerous goods via different modes of transport. These organizations have developed legal regulations, instruments and recommendations for safety and security (see paras 7.6–7.17), which are often adopted by States for the purpose of domestic transport.

Transport by sea

7.6. Under the auspices of the International Maritime Organization, international conventions and guidance address the transport security of dangerous goods,

including nuclear and other radioactive material, in the maritime domain. Instruments that are pertinent to maritime security considerations are the International Convention for the Safety of Life at Sea [34] and its three annexes: the International Ship and Port Facility Security Code [35], the International Maritime Dangerous Goods Code [6] and the International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships [36].

International Maritime Dangerous Goods Code

7.7. Maritime shipments of nuclear and other radioactive material are subject to the International Maritime Dangerous Goods Code [6], which requires that certain elements of security awareness relating to dangerous goods be included in training for crew members. Crew members involved in the shipment of dangerous goods should thus be familiar with the provisions of relevant security plans commensurate with their responsibilities. The focus of the Code [6] is on the security of the material being shipped, rather than on maritime security elements such as vessels or port facilities.

7.8. Key provisions of the International Maritime Dangerous Goods Code [6] reference existing international requirements, including IAEA recommendations for the transport security of nuclear material by sea, ensuring alignment between requirements of the Code and the recommendations provided in Refs [2, 4].

International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships

7.9. The International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships [36] requires that certain shipments of nuclear material be transported on specially designed vessels. Further information on the classification of ships is provided in the Code [36].

7.10. The International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships [36] uses a graded approach to vessel classification for certain safety features of the vessel design and on-board equipment, but these features are not related to nuclear security. They may, however, support overall transport security. Measures specific to transport security should be applied using a graded approach, on the basis of existing IAEA publications (see Refs [2, 4]).

International Ship and Port Facility Security Code

7.11. The International Ship and Port Facility Security Code [35] establishes security requirements and recommendations during maritime transport for both vessels and port facilities, as well as the personnel involved in operations. These requirements and recommendations apply to international voyages for maritime transport and domestic short sea shipping within a State's jurisdictional limits.

7.12. The International Ship and Port Facility Security Code [35] requires that a vessel security officer be assigned to each vessel during its voyage. The vessel security officer is responsible for the maritime security of the vessel during its operation, and this person is aware of all of the cargo on board. When a transport security plan is drafted, it should be consistent with the content of the security plans provided in the Code [35], and the vessel security officer should be consulted regarding its content and the associated measures applicable to the maritime leg of the voyage.

7.13. The International Ship and Port Facility Security Code [35] requires the preparation of a vessel security plan and a facility security plan. These plans may be referenced or included in the transport security plan. Both the vessel security plan and the facility security plan may include additional requirements for monitoring and controlling the access and activities of authorized persons on the vessel and at the port facility, including the determination of trustworthiness. In addition, the vessel security plan and facility security plan include security measures such as the availability of communications and associated systems.

7.14. In cases where the shipment of nuclear or other radioactive material is undertaken through domestic short sea shipping or other short voyages, and the ship needs to pass through a port facility without established security areas for dangerous goods, temporary security measures should be applied. If agreed by the relevant competent authorities within the State, these temporary security measures (e.g. establishment of restricted areas with access control, use of guards) should be implemented through a graded approach.

Transport by air

7.15. The International Civil Aviation Organization adopted new international standards and recommended practices on aviation security, provided in annex 17 to the Convention on International Civil Aviation [37] (also known as the Chicago Convention), to address security in civil aviation, including in airports.

7.16. The International Air Transport Association has also published a security manual [38] outlining principles that are to be respected by commercial airlines in order to build effective aviation security.

7.17. General training in the application of the security provisions of the International Civil Aviation Organization or the International Air Transport Association would be beneficial for understanding how to ensure the effective security of nuclear and other radioactive material when using this mode of transport.

MANAGEMENT OF SAFETY AND SECURITY INTERFACES DURING TRANSPORT

7.18. Paragraph 1.2 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [39] states that "Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment." Nonetheless, the activities that address nuclear safety and nuclear security may differ. At times, actions taken to strengthen nuclear safety might have either a positive or a negative effect on nuclear security.

7.19. According to para. 1.10 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [40], "Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security." In accordance with SSR-6 (Rev. 1) [13], security measures and safety measures for the transport of nuclear and other radioactive material are required to be implemented in a coordinated manner. Other regulations, standards, codes and guides developed for transport safety purposes could influence the design and implementation of the transport security system of a shipper or carrier.

7.20. Competent authorities should therefore establish a well coordinated approach to manage the interface between nuclear safety and nuclear security for nuclear and other radioactive material in transport so that relevant measures are implemented in a manner that does not compromise or negatively impact either nuclear safety or nuclear security. The aim should be to manage this interface in a way that capitalizes on improving mutual awareness and understanding while providing opportunities for mutual enhancement of both transport safety and transport security.

Administrative management of safety and security interfaces

7.21. When a shipper is in the process of developing a plan to move material safely, it is best practice to also plan for the security of this material during transport. Planning and coordination should therefore be organized among the different functional entities responsible for safety, emergency response, security and law enforcement.

7.22. In certain circumstances, there may be a conflict between the information requirements associated with security and safety — notably, when sharing information relating to the operational aspects of a shipment (e.g. the transport security plan) or to authorizations (e.g. the transport licence application). For safety reasons, and often for regulatory compliance purposes, various stakeholders might receive information about the shipment; for example, the type of material being transported, the day of departure and the shipment's planned route. This information is transmitted so that government agencies with jurisdiction over the shipment (e.g. licensing agencies) or those along the route (e.g. security escort agencies) can properly plan and support the shipment. However, for security purposes, such information should only be shared on a need to know basis and in such a way as to protect the information from potential adversaries. The shipper and competent authorities should apply a risk informed approach to handling and transmitting the necessary information. They should also assess what information needs to be shared when, how and with whom so that it does not present a security risk. At the same time, the shipper and competent authorities should ensure that the information is shared in a way that meets all of the national safety requirements.

7.23. Other examples of areas where the interfaces between safety measures and security measures may need to be managed are as follows:

(a) Safety and security inspections;
(b) Design of transport packages;
(c) In-transit storage;
(d) Communication;
(e) Written instructions and documentation;
(f) Marking and labelling of packages and placarding of vehicles and freight containers;
(g) Development and implementation of compensatory measures;
(h) Implementation of transport operations;
(i) Response arrangements during temporary storage or handover from one jurisdiction to another.

7.24. These interfaces, and possible ways to address challenges in the management of the safety–security interface, are described in Ref. [15] for commercial shipments of radioactive material. The information provided in Ref. [15] may also be valid for a broader range of nuclear and other radioactive material in transport and thus could be applied accordingly.

Package design

7.25. For shipments of radioactive material, the Model Regulations [5] — harmonized with SSR-6 (Rev. 1) [13] since 2021 — establish design requirements for transport packages using a graded approach. For normal commercial shipments of radioactive material, these packages could include excepted packages with the least robust design, industrial and Type A packages of moderately robust design, or Type B packages with the most robust design. In some cases, the robustness of the package, designed for safety purposes for the containment of material and control of external radiation levels, might also provide security benefits during transport.

7.26. Type B packages that are used for transporting large quantities and high activities of irradiated materials are often large in size (e.g. transport casks). A Type B package for spent nuclear fuel may weigh up to 130 000 kilograms. Their large mass makes unauthorized removal from the transport conveyance very complicated, necessitating the use of specialized lifting and handling equipment.

7.27. Type B packages are designed to provide resistance to high impact and fire, as well as radiation shielding. These packages are designed to ensure that the material being transported does not present a significant radiation hazard and does not release its contents, even in a severe accident. For this reason, Type B package designs should demonstrate an ability to withstand tests simulating normal shipping conditions and tests simulating severe accident conditions, without the release of contents and without a significant increase in external radiation levels.

Security overpacks and freight containers

7.28. A shipper might use additional security equipment beyond that indicated in the approved package design, such as overpacks. Overpacks are used to enclose one or more packages of nuclear or other radioactive material in a single handling unit. Shippers may use overpacks for several purposes, such as to consolidate a number of packages into a single handling unit for simpler and quicker loading, or to enhance the security of the package by providing additional delay features. Overpacks can be open or closed, may have special features to facilitate industrial

handling equipment or may incorporate unique locking mechanisms. They can also be configured for use on specific types of conveyance.

7.29. The use of overpacks and freight containers should be considered when designing the package and the conveyance and when evaluating their overall safety and security effectiveness. Overpacks and freight containers can provide increased protection against fire or collision and can delay the unauthorized removal of material and packages. The use or incorporation of overpacks may necessitate a safety review of the package design, however, to ensure that the overpack does not adversely affect the safety features of the package.

7.30. Some safety control measures could be enhanced to serve also as security measures. For example, a fastening device that cannot be unintentionally opened could be fitted to the containment system, or the package tie-down attachments could be secured with locks, to provide delay and to deter attempted removal of the package from the conveyance.

Package seals

7.31. In many instances and for many package designs, regulations require the use of seals (e.g. tamper indicating devices), which are not readily breakable and, when they are intact, provide evidence that the package has not been opened or breached. Seals may also be installed on packages containing nuclear material for safeguards purposes. Seals may also fulfil security functions (e.g. inventory verification), since many seals are uniquely identified with a specific alphanumeric code. Paragraphs 5.8–5.16 provide more detailed guidance on package seals.

Maritime tracking

7.32. Maritime safety regulations, such as those outlined in the International Convention for the Safety of Life at Sea [34], require automated communications systems that provide information on a vessel's identity, type, position, course, speed, navigational status and other safety related information.

7.33. The use of an automatic identification system for maritime transport presents an example of a transport safety and transport security challenge. The automatic identification system is used primarily to provide the user with navigational information regarding vessels in the vicinity. This information supplements information obtained from the radar; for example, the distance of the nearest point of approach of a vessel or the time of the nearest point of approach. The automatic identification system is designed to provide positive identification of a

vessel for communication purposes. However, for security purposes, and in some locations around the world, vessels might not wish to identify themselves. The safety and security implications should thus be carefully weighed when deciding to deactivate the automatic identification system, and the relevant sections of the International Convention for the Safety of Life at Sea [34] should be closely consulted in this regard.

REFERENCES

[1] 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), https://doi.org/10.61092/iaea.ko2c-dc4q

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[5] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE, Recommendations on the Transport of Dangerous Goods, Model Regulations, Twenty-second revised edition, ST/SG/AC.10/1/Rev. 22 (Vols I and II), UN, New York and Geneva (2021), https://doi.org/10.18356/9789210052191

[6] INTERNATIONAL MARITIME ORGANIZATION, International Maritime Dangerous Goods Code, IMO, London (2022).

[7] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Technical Instructions for the Safe Transport of Dangerous Goods by Air (Doc 9284), ICAO, Montreal (2023/2024).

[8] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE, European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR), 2021 Edition, UNECE, New York and Geneva (2020).

[9] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE, INLAND TRANSPORT COMMITTEE, European Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN), 2021 Edition, UNECE, Geneva (2020).

[10] INTERGOVERNMENTAL ORGANISATION FOR INTERNATIONAL CARRIAGE BY RAIL, Regulations Concerning the International Carriage of Dangerous Goods by Rail (RID), 2023 Edition, OTIF, Berne (2023).

[11] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[12] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1/Mod. 1 (Corrected), IAEA, Vienna (2021).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, IAEA Safety Standards Series No. SSR-6 (Rev. 1), IAEA, Vienna (2018), https://doi.org/10.61092/iaea.ur52-my9o

[14] EUROPEAN COMMISSION, 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 ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014), https://doi.org/10.61092/iaea.u2pu-60vm

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Managing the Interface Between Safety and Security for Normal Commercial Shipments of Radioactive Material, Technical Reports Series No. 1001, IAEA, Vienna (2021).

[16] 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, Nuclear Security Series No. 15, IAEA, Vienna (2011).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency Involving the Transport of Radioactive Material, IAEA Safety Standards Series No. SSG-65, IAEA, Vienna (2022).

[18] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015), https://doi.org/10.61092/iaea.3dbe-055p

[19] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, 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).

[20] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, 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).

[21] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR OFFICE, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Arrangements for the Termination of a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-11, Vienna (2018).

[22] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERPOL, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION AND UNITED NATIONS OFFICE FOR OUTER SPACE AFFAIRS, Arrangements for Public Communication in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-14, Vienna (2020).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

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

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

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material (2018 Edition), IAEA Safety Standards Series No. SSG-26 (Rev. 1), IAEA, Vienna (2022), https://doi.org/10.61092/iaea.qz7d-jiym

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

[30] GARCIA, M.L., The Design and Evaluation of Physical Protection Systems, 2nd edn, Butterworth Heinemann, Burlington, MA (2008), https://doi.org/10.1016/C2009-0-25612-1

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Security of Nuclear and Other Radioactive Material in Transport, Non-serial Publications, IAEA, Vienna (2018).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA,Vienna (2020).
[34] INTERNATIONAL MARITIME ORGANIZATION, International Convention for the Safety of Life at Sea, IMO, London (1974).
[35] INTERNATIONAL MARITIME ORGANIZATION, International Ship and Port Facility Security Code, IMO, London (2014).
[36] INTERNATIONAL MARITIME ORGANIZATION, International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High Level Radioactive Wastes on Board Ships (INF Code), IMO, London (1999).
[37] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Annex 17 to the Convention on International Civil Aviation Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference, Twelfth Edition, ICAO, Montreal (2022).
[38] INTERNATIONAL AIR TRANSPORT ASSOCIATION, Security Management System Manual, IATA, Montreal (2021).
[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013),
https://doi.org/10.61092/iaea.ajrj-ymul
[40] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006),
https://doi.org/10.61092/iaea.hmxn-vw0a

IAEA
International Atomic Energy Agency

No. 27

ORDERING LOCALLY

IAEA priced publications may be purchased from our lead distributor or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA.

Orders for priced publications

Please contact your preferred local supplier, or our lead distributor:

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

Trade orders and enquiries:
Tel: +44 (0)1235 465576
Email: trade.orders@marston.co.uk

Individual orders:
Tel: +44 (0)1235 465577
Email: direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

For further information:
Tel. +44 (0) 207 240 0856
Email: info@eurospan.co.uk
www.eurospan.co.uk

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

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530
Email: sales.publications@iaea.org
www.iaea.org/publications

This publication provides detailed guidance to States and their competent authorities on how to implement and maintain a nuclear security regime for the transport of nuclear and other radioactive material. The publication builds upon relevant recommendations in IAEA Nuclear Security Series Nos 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), and 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, and provides additional explanations of how to implement these recommendations in practice. This publication is intended for nuclear security regulatory bodies and may also be useful to operators, shippers, carriers and others with transport security responsibilities to design their transport security systems.

International Atomic Energy Agency
Vienna, 2024
www.iaea.org