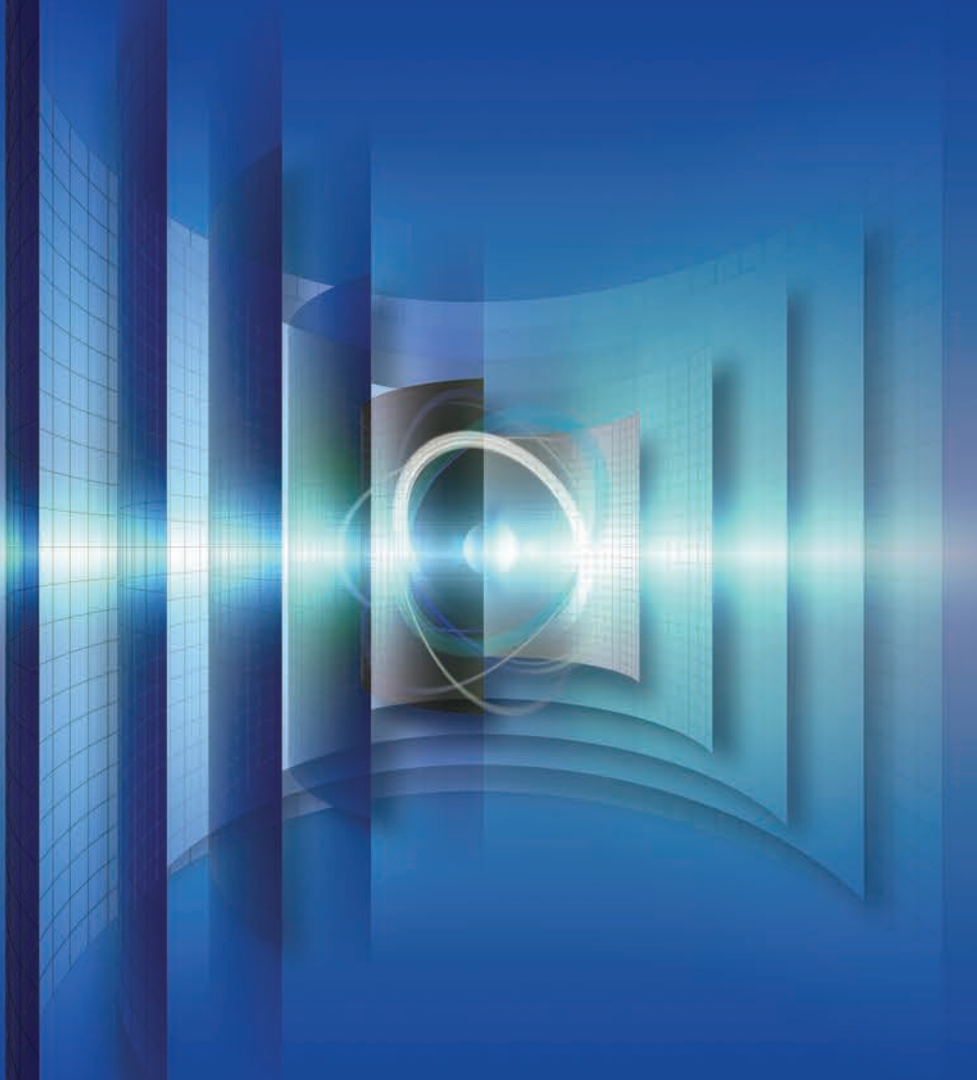
IAEA Nuclear Security Series No. 9-G (Rev. 1)

Implementing Guide

Security of Radioactive Material in Transport



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

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

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

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

SECURITY OF 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
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
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
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 LUCIA
SAINT VINCENT AND THE GRENADINES
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
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
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. 9-G (Rev. 1)

SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2020

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
July 2020
STI/PUB/1872

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Security of radioactive material in transport / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2020. | Series: IAEA nuclear security series, ISSN 1816-9317 ; no. 9-G (Rev. 1) | Includes bibliographical references.
Identifiers: IAEAL 20-01297 | ISBN 978–92–0–105119–6 (paperback : alk. paper) | ISBN 978–92–0–158419–9 (pdf)
Subjects: LCSH: Radioactive substances — Transportation. | Hazardous substances — Transportation. | Transportation — Security measures.
Classification: UDC 656.073.436 | STI/PUB/1872

FOREWORD

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

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

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

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

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

EDITORIAL NOTE

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance for States to assist them in implementing a national nuclear security regime and in reviewing, and when necessary strengthening, this regime. The series also provides guidance for States to fulfil their obligations and commitments with respect to binding and non-binding international instruments. The Nuclear Security Fundamentals set out the objective of a nuclear security regime and its essential elements in IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1]. The IAEA Nuclear Security Recommendations indicate what a nuclear security regime should address in IAEA Nuclear Security Series Nos 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2]; 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3]; and 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [4].

1.2. This Implementing Guide supports Ref. [3].

1.3. This publication supersedes IAEA Nuclear Security Series No. 9, Security in the Transport of Radioactive Material, which was issued in 2008.[1] This revision was undertaken to better align this Implementing Guide with Ref. [3], which was published in 2011, to cross-reference other relevant Implementing Guides published since 2008, and to add further detail on certain topics based on the experience of the IAEA and its Member States in using the previous version.

1.4. This Implementing Guide also takes into account the robust international framework of guidance on the international transportation of dangerous goods, including radioactive material. The United Nations (UN) Model Regulations [5] provide a basis for States to develop security requirements for the transport of all dangerous goods. In some cases, the UN Model Regulations [5] are implemented directly by States. They are also used by international modal organizations (those organizations that focus on a particular mode of transport). The security provisions for the transport of dangerous goods are found in Chapters 1.4 and 7.2 of the UN Model Regulations [5]. Other UN specialized agencies and

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

programmes have taken similar steps to support improved security in the transport of all dangerous goods. The International Maritime Organization, International Civil Aviation Organization, United Nations Economic Commission for Europe, Intergovernmental Organization for International Carriage by Rail and European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways have all amended their respective international instruments [6–10] to reflect the security provisions of the UN Model Regulations [5].

1.5. The Convention on the Physical Protection of Nuclear Material and its Amendment [11–13] provide an international framework for ensuring the physical protection of nuclear material used for peaceful purposes, including while in international transport. The Convention and its Amendment also apply, with certain exceptions, to nuclear material while in domestic use, storage and transport.

1.6. The IAEA has established requirements for the safety of radioactive material during transport in the IAEA Safety Standards Series. The relevant publications include IAEA Safety Standards Series Nos SSR-6 (Rev. 1), Regulations for the Safe Transport of Radioactive Material [14]; SF-1, Fundamental Safety Principles [15]; and GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [16].

OBJECTIVE

1.7. The objective of this publication is to provide guidance to States and their competent authorities on how to establish and maintain the elements of the nuclear security regime relating to the transport of radioactive material. This publication may also assist shippers, carriers and others with transport security responsibilities in designing their security systems.

1.8. This publication is intended to facilitate the establishment of an internationally consistent approach to security of radioactive material in transport in States. This publication builds on the relevant recommendations in Ref. [3] and provides additional guidance on how to implement these recommendations in practice.

SCOPE

1.9. This publication applies to the security of packages containing radioactive material that could cause unacceptable radiological consequences if used in a

malicious act during international and domestic transport. It also applies to the security of some nuclear materials of Category III and below during transport, owing to the radioactive nature of the material. This publication provides guidance for protection against unauthorized removal and sabotage.

1.10. This publication also describes arrangements and measures to locate and recover lost, missing or stolen radioactive material. More detailed guidance on this topic can be found in Ref. [4]. This publication does not address emergency preparedness and response aspects of a nuclear security event involving radioactive material in transport. These topics are covered in other IAEA publications [17–20].

1.11. Security and safety measures for transport of radioactive material should be implemented in a coordinated manner to comply with Ref. [14] as well as with relevant IAEA safety standards and nuclear security guidance. Other regulations, standards, codes and guides developed for safety purposes might also apply and could influence the design and implementation of the transport security system of a shipper or carrier. IAEA Safety Standards Series publications state that "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" [15].

1.12. The transport security measures proposed in this publication are complementary to the provisions in Ref. [2] and its supporting Implementing Guide, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G [21]. This publication does not apply to the physical protection of nuclear material in transport against unauthorized removal for use in a nuclear explosive device as this is addressed in Ref. [2] and its supporting Implementing Guide [21]. However, this publication does apply to the physical protection of nuclear material in transport where the risk with respect to a potential malicious act is owing to the material's radioactivity rather than its fissile properties. Notably, because of their radioactivity, some Category III and below Category III nuclear material packages might warrant more stringent security measures than those specified by Ref. [21] if the methodology described in this publication is applied.

1.13. This publication also provides guidance on the implementation of transport security measures contained in the Code of Conduct on the Safety and Security of Radioactive Sources (hereinafter referred to as the Code of Conduct) [22] and its supplementary document, Guidance on the Import and Export of Radioactive Sources [23].

1.14. While the guidance presented in this publication is consistent with the UN Model Regulations [5], some specific security measures are complementary to those in the UN Model Regulations.

1.15. Many States have taken into account the guidance in the superseded 2008 Implementing Guide in establishing regulatory requirements. This revised Implementing Guide may be useful to regulatory bodies by providing additional guidance to shippers and carriers.

STRUCTURE

1.16. This publication follows the structure of Ref. [3]. Section 2 summarizes the objectives of the elements of a State's nuclear security regime for transport of radioactive material and provides guidance on implementing these elements. Section 3 describes the characterization of radioactive material for the application of appropriate security measures during transport. Section 4 provides guidance on the establishment of a regulatory programme for transport security, including the specification of roles and responsibilities. Section 5 provides guidance on security measures to be taken to protect against unauthorized removal and sabotage during transport. Section 6 provides guidance on measures to be used to locate and recover missing or stolen radioactive material. Appendix I provides background information on the establishment of activity threshold values for transport security measures. Appendix II provides information on the development of a transport security plan. Annex I provides an example transport security plan and describes its content and structure. Annex II provides a sample checklist for transport security verification of a shipment. Annex III provides a cross-reference of mode independent security measures to where they are discussed within this publication.

2. ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME RELATING TO TRANSPORT OF RADIOACTIVE MATERIAL

2.1. Paragraph 2.1 of Ref. [3] states:

> "The overall objective of a State's *nuclear security regime* is to protect persons, property, society, and the environment from *malicious acts*

involving *nuclear material* or other radioactive material that could cause *unacceptable radiological consequences*. The objectives of a *nuclear security regime* for *radioactive material*, *associated facilities* and *associated activities* should be:

— Protection against *unauthorized removal* of *radioactive materia*l used in *associated facilities* and in *associated activities*;
— Protection against *sabotage* of *other radioactive material*, *associated facilities* and *associated activities*;
— Ensuring the implementation of rapid and comprehensive measures to locate, recover, as appropriate, *radioactive material* which is lost, missing or stolen and to re-establish regulatory control.

The third objective is mainly related to *radioactive material* out of *regulatory control*, which is addressed in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [Ref. [4]]."

2.2. Paragraph 2.2 of Ref. [3] states:

"These objectives are realized through security measures to deter, detect, delay and respond to a potential *malicious act*, and to provide for the security management of *radioactive material* and *associated facilities* and *associated activities*."

2.3. Paragraph 2.3 of Ref. [3] states:

"These security measures should be based on a risk informed *graded approach* so that similar security is provided for material capable of resulting in similar potential radiological consequences arising from use in a *malicious act*. They should also use the concept of *defence in depth*."

2.4. Paragraph 2.4 of Ref. [3] states:

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

2.5. Each of these objectives applies to the protection of radioactive material in transport as well as to nuclear material in use and storage (addressed in Ref. [2]).

2.6. This section addresses the elements of a State's nuclear security regime relating to the transport of radioactive material used to achieve these objectives.

STATE RESPONSIBILITY

2.7. Paragraph 3.1 of Ref. [3] states that "The responsibility for the establishment, implementation and maintenance of a *nuclear security regime* within a State rests entirely with that State."

2.8. Transport security should be an integral part of the State's overall security regime for radioactive material. Each State has a responsibility to regulate radioactive material in transport in order to protect this material from malicious acts that could result in radiological consequences to persons, property, society and the environment. Responsibility rests entirely with the State to ensure that its security regime provides an effective framework for the protection of radioactive material under its jurisdiction.

2.9. Paragraph 3.2 of Ref. [3] states:

> "The State should clearly define and assign nuclear security responsibilities to *competent authorities*, noting that they may include *regulatory bodies*, law enforcement, customs and border control, intelligence and security agencies, health agencies, etc. Provision should be made for appropriate integration and coordination of responsibilities within the State's *nuclear security regime*. Clear lines of responsibility and communication should be established and recorded between the *competent authorities*."

2.10. The State's nuclear security regime should include the following elements with respect to transport security of radioactive material:

(a) Provisions in the legislative and regulatory framework governing the security of the radioactive material in transport;
(b) Competent authorities, including a regulatory body responsible for implementing the relevant provisions of the legislative and regulatory framework;
(c) Transport specific security systems and measures.

2.11. The elements of the State's security regime applicable to security of radioactive material in transport should be reviewed and, if necessary, updated regularly by the competent authorities.

2.12. The State should ensure that the regulatory body responsible for the security of radioactive material in transport has effective independence. Organizational units responsible for licensing and supervisory activities should have appropriate, sufficient and unfettered discretion in the execution of their tasks, and other government agencies or external organizations should not have undue influence on the execution of licensing and supervisory tasks.

2.13. If the responsibility for the security of radioactive material in transport is divided between two or more competent authorities, arrangements should be made for overall coordination. Clear lines of responsibility between these entities should be established and recorded to ensure continuous protection of the material.

2.14. Paragraph 3.3 of Ref. [3] states:

> "The State should ensure effective overall cooperation and relevant information sharing between the *competent authorities*. This should include sharing of relevant information (such as information about the *threat* to be protected against and other useful intelligence) in accordance with national regulations."

2.15. States should establish appropriate mechanisms for international cooperation, consultation and information exchange on security techniques and practices for transport, within the constraints of confidentiality. States should assist each other in recovering stolen or missing radioactive material when requested. Appropriate arrangements may be established between shipping, receiving and transit States, and relevant intergovernmental organizations to promote cooperation, consultation and information exchange, and to ensure that radioactive material under their jurisdiction is adequately protected.

2.16. The State's security contingency plans at the national level should include a description of response measures that the State will undertake in the event of actual or attempted unauthorized removal or sabotage of radioactive material or packages containing such material (referred to in the remainder of the publication simply as 'packages') during domestic and international transport. These measures should be coordinated with the State emergency plans for response to a nuclear or radiological emergency consistent with the all hazards approach [2, 21].

INTERNATIONAL TRANSPORT

2.17. Paragraph 4.38 of Ref. [3] states that "For international transport, *shippers* and/or carriers should ensure in advance that any State by State variations in security requirements are applied and should determine the point at which the responsibility for security is transferred."

2.18. The State should require that radioactive material on ships and aircraft registered to that State is adequately protected while in international waters or airspace and until responsibility is transferred to another State.

2.19. The importing State and the exporting State should coordinate prior to transport of radioactive material to reduce the likelihood of malicious acts in connection with the import or export of radioactive material. At a minimum, the coordination should be consistent with paras 23–29 of Ref. [22] for Category 1 and 2 radioactive sources.

2.20. International shipments might involve land transport by road or rail, intermodal transfers, transport by aircraft or ship, transit through multiple States and in-transit storage. The regulatory body should require the shipper and carrier to maintain the security of the radioactive material throughout transport and to clearly define how any transfer of security responsibilities for the material will occur.

LEGISLATIVE AND REGULATORY FRAMEWORK

State

2.21. Paragraph 3.4 of Ref. [3] states:

> "The State should establish, implement and maintain an effective national legislative and regulatory framework to regulate the nuclear security of *radioactive material*, *associated facilities* and *associated activities*, which:
>
> — Takes into account the risk of *malicious acts* involving *radioactive material* that could cause *unacceptable radiological consequences*;
> — Defines the *radioactive material*, *associated facilities* and *associated activities* which are subject to the *nuclear security regime* in terms of nuclides and quantities of *radioactive material* present;
> — Prescribes and assigns governmental responsibilities to relevant entities including an independent *regulatory body*;

— Places the prime responsibility on the *operator, shipper* and/or carrier for implementing and maintaining security measures for *radioactive material*;
— Establishes the *authorization* process for *radioactive material*, *associated facilities* and *associated activities*. As appropriate, the *authorization* process concerning the security of *radioactive material* could be integrated within one defined for safety or radiation protection;
— Establishes the inspection process for security requirements;
— Establishes the enforcement process for the failure to comply with security requirements established under legislative and regulatory framework;
— Establishes sanctions against the *unauthorized removal* of *radioactive material* and *sabotage* of *associated facilities* and *associated activities*;
— Takes into account the interface between security and safety of *radioactive material*."

2.22. The above applies to radioactive material in transport as well as in use and storage. In addition, to address the secure transport of radioactive material, the national legislative and regulatory framework should do the following, in accordance with a graded approach and where applicable:

(a) Establish an authorization process specific to radioactive material in transport, which may include issuance of specific licences or other forms of authorization;
(b) Establish a procedure for submission of a transport security plan by the shipper and carrier and, as appropriate, for approval of the plan by the competent authority prior to transport;
(c) Prescribe requirements for the design and evaluation of the transport security system by the shipper and carrier, as appropriate;
(d) Include provisions for the regular review of the transport security requirements to take into account advances in technology and potential changes in the threat;
(e) Establish a programme that verifies continued compliance with transport security requirements through periodic inspections and reviews, and ensures that corrective actions are taken when needed;
(f) Establish a policy to identify, classify and control sensitive information relating to transport security, the unauthorized disclosure of which could compromise the security of radioactive material in transport;
(g) Include requirements, consistent with national practices, for ensuring the trustworthiness of persons with authorized access to sensitive information or to radioactive material during transport or who have specific security

responsibilities during transport and establish trustworthiness verification and security clearance procedures for such persons commensurate with their responsibilities (e.g. requirements for positive identification of such persons);

(h) Establish requirements for reporting of security related events, including missing or lost packages of radioactive material.

2.23. Within the legal and regulatory framework, each State should clearly assign security responsibilities to the shipper, carrier, receiver or others engaged in the transport of radioactive material. For example, the State might choose to hold the shipper solely responsible for security during transport by requiring that the shipper either conduct the transport operation or use a carrier that implements security measures under the direction of the shipper. The State might also choose to assign the responsibilities for security to carriers who are authorized by the competent authority to securely transport radioactive material, and permit the shipper to rely on the carrier's security system. Typical responsibilities assigned by the State include developing a transport security plan, providing advance notification of the shipment details to the receiver and completing other relevant technical, procedural and administrative activities.

2.24. The State's legislative and regulatory framework should also specify the requirements for contingency planning by shippers, carriers and receivers, including requirements for coordination with State and local authorities.

Regulatory body

2.25. Paragraph 3.11 of Ref. [3] states:

> "The *regulatory body* should implement the legislative and regulatory framework and authorize activities only when they comply with its nuclear security regulations. Where it is required, the security plan…can be used by the regulatory body in its determination for issuance of an authorization."

2.26. The regulatory body responsible for transport security should implement the relevant elements of the legislative and regulatory framework and authorize transport activities only when they comply with the framework's regulations. When the applicant is required to submit a transport security plan, the review of the transport security plan can be used by the regulatory body to determine whether to issue an authorization.

2.27. The regulatory body should have a clearly defined legal status; independence from shippers, carriers, receivers and others involved in transport; and the legal authority and capabilities needed to perform its responsibilities and functions effectively.

2.28. The regulatory body should verify continued compliance with transport security regulations and, as appropriate, relevant authorization conditions through inspections and reviews. It should also require that shippers and carriers take corrective action when a requirement is not met. Inspections of security measures implemented by shippers, carriers and receivers could be coordinated with inspections by other regulatory bodies responsible for verifying compliance with other regulatory requirements, such as those for radiation protection and safety, taking into account the need for protection of sensitive information.

2.29. The responsibilities of the regulatory body with respect to transport security should include the following:

(a) Establishing requirements for security during the transport of radioactive material based on the national threat assessment, the design basis threat or alternative threat statement (see para. 2.45). The IAEA Nuclear Security Series Nos 10-G (Rev. 1), National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements [24]; and 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [25], can be used, as applicable, in order to protect against unauthorized removal and sabotage.
(b) Establishing requirements for the content and submission of transport security plans, if required.
(c) Licensing or otherwise authorizing shippers and carriers to transport radioactive material when such a licence or other form of authorization is required.
(d) Performing inspections (both announced and unannounced) and reviews of radioactive material shipments as needed to ensure that the shipments are undertaken in compliance with the applicable requirements and conditions established by the regulatory body.
(e) Performing evaluations of the transport security systems implemented by operators consistent with a graded approach and including exercises, where appropriate, depending on the regulatory approach chosen by the State.
(f) Establishing requirements for shippers and carriers to perform trustworthiness checks for all personnel with security responsibilities during transport of radioactive material or access to sensitive information, using a graded approach.

(g) Establishing which transport related information should be considered as sensitive information and ensuring that its confidentiality is protected accordingly, including within the regulatory body itself.
(h) Enforcing applicable requirements, including those regarding the taking of corrective actions when needed.
(i) Liaising with other competent authorities, in particular those responsible for transport safety and import and export control.

2.30. The responsibilities described in this subsection as well as others assigned to the regulatory body could be performed by the regulatory body in cooperation with other competent authorities.

Shipper, carrier and receiver

2.31. Paragraph 3.13 of Ref. [3] states:

> "The legislative and regulatory framework should require that the *operator*, *shipper* and/or carrier:
>
> — Comply with all applicable regulations and requirements established by the State and the *regulatory body*;
> — Implement security measures that comply with requirements established by the State and the *regulatory body*;
> — Establish quality management programmes that provide:
> • Assurance that the specified requirements relating to nuclear security are satisfied;
> • Assurance that the components of the *nuclear security system* are of a quality sufficient for their tasks;
> • Quality control mechanisms and procedures for reviewing and assessing the overall effectiveness of security measure;
> — Report to the *regulatory body* and/or to any other *competent* authority, all *nuclear security events* involving *radioactive material*, *associated facilities* and *associated activities* according to national practices;
> — Cooperate with and assist any relevant *competent authorities* in case of a *nuclear security event*."

2.32. The above recommendations drawn from Ref. [3] should also be considered to apply to receivers, as appropriate.

2.33. The legislative and regulatory framework should ensure that these general measures explicitly include transport security. In particular, the regulatory body

should ensure that security measures implemented by the shipper, carrier and receiver are operational and that all necessary permits and authorizations have been obtained prior to the commencement of transport.

2.34. The regulatory framework should clearly allocate transport security responsibilities to the shipper, carrier and receiver. When the shipper relies on the carrier or receiver to perform security functions assigned to the shipper, these functions should be specified in the contractual arrangements between the shipper and the carrier or receiver. Any transfers of security responsibilities between the shipper, the carrier, the receiver and others engaged in the transport of radioactive material should be clearly specified and agreed to before the transport is undertaken.

2.35. When authorized by the State, the receiver can be assigned responsibility for implementing security measures in certain cases. For example, for import shipments, the receiver might have the primary responsibility for implementing security measures for radioactive material once the shipment arrives in the importing State.

2.36. The carrier should ensure that its activities are in compliance with applicable national regulations. These might include the following:

(a) Providing a conveyance and crew that complies with all applicable safety and security requirements, including crew fitness for duty (e.g. trustworthiness, drug testing, training and licensing), conveyance suitability and maintenance requirements;
(b) Ensuring that any equipment provided by the carrier is suitable for the application intended and satisfies regulatory requirements;
(c) Ensuring that, if an incident occurs during transport, carrier personnel are prepared to act in accordance with the emergency and contingency plans.

Subcontracting

2.37. The regulatory body should require that, if subcontractors are used during the shipment, the contracting party (whether the shipper or carrier) ensures that the subcontractor is fully aware of applicable security requirements. The contracting party should also verify that appropriate security arrangements are maintained throughout the shipment. If a licence or other form of authorization is required to perform transport activities, the contracting party should ensure that its subcontractor is duly licensed or otherwise authorized.

Deficiencies

2.38. The regulatory body should require that, if deficiencies are discovered in the transport security system prior to shipment, the shipper or carrier correct the deficiencies or implement immediate compensatory measures to ensure appropriate protection for the shipment before starting the transport activities.

2.39. If deficiencies are discovered by the crew during transport, the regulatory body should require that they be reported immediately to the management of the shipper or carrier and that compensatory measures be taken to ensure appropriate protection for the shipment.

ASSESSMENT OF TRANSPORT SECURITY THREATS

2.40. Paragraph 3.17 of Ref. [3] states:

> "The State should assess its national *threat* for *radioactive material*, *associated facilities* and *associated activities*. The State should periodically review its national *threat*, and evaluate the implications of any changes in the *threat* for the design or update of its *nuclear security regime*."

2.41. Paragraph 3.18 of Ref. [3] states:

> "The *regulatory body* should use the results of the *threat assessment* as a common basis for determining security requirements for *radioactive material* and for periodically evaluating their adequacy. The *regulatory body* should have access to information from other State authorities on present and foreseeable *threats* involving *radioactive material*."

2.42. In particular, the State should assess and periodically review its national threat for radioactive material in transport and evaluate the implications of any changes in the threat [3].

2.43. The regulatory body should require that shippers, carriers and receivers implement security measures appropriate to counter the national threat. Additionally, the regulatory body may choose to communicate threat information, including changes in the threat, to the shipper, carrier and receiver to aid in the development of their security systems and transport security plans. Such information should be appropriately protected owing to its sensitive nature.

2.44. As discussed in Ref. [24], States will vary in their capabilities for identifying and evaluating threat information. Sources of information for the national threat assessment should include intelligence agencies as well as ministries of interior, defence, transportation and foreign affairs, law enforcement, customs, coast guard and other agencies with security related responsibilities. The regulatory body or bodies may also participate in the threat assessment process. The national threat assessment should be updated on a regular basis or when the circumstances make it necessary, for example, when new information pertaining to criminal activity is acquired.

2.45. One method for using threat information when establishing regulatory requirements is to apply the national threat assessment directly. Alternatively, the national threat assessment can be used to develop and apply a design basis threat or an alternative threat statement, which the regulatory body could adapt and use in developing regulatory requirements. Further guidance on threat assessment, on defining a design basis threat or an alternative threat statement based on a threat assessment, and considerations concerning the decision of whether to use a design basis threat or an alternative threat statement is given in Refs [2] and [25].

2.46. The regulatory body should provide guidance to the shipper, carrier, receiver and others engaged in transport of radioactive material on recognizing the potential for insider threats within their organizations. Security systems should be designed, in a graded manner, to protect against the insider threat, particularly for personnel that exercise control over a shipment (such as a truck driver). More information relating to insider threats may be found in IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [26].

RISK INFORMED TRANSPORT SECURITY SYSTEMS AND MEASURES

2.47. Establishing risk informed transport security systems and measures involves taking into account risk management, applying a graded approach and defence in depth, specifying risk informed security provisions and ensuring a coordinated approach to the safety–security interface. Each of these areas is addressed in the following subsections.

Risk management

2.48. The State should use a risk management approach to maintain the risk of unauthorized removal or sabotage during transport at an acceptable level. Such an

approach includes evaluating the threat and potential consequences of malicious acts and ensuring that appropriate security measures are in place to protect against such acts.

2.49. The State should decide what level of risk is acceptable and what level of effort is justified to protect radioactive material in transport against the threat defined in the national threat assessment, with the goal of reducing the risk associated with the shipment to an acceptable level. The level of risk judged to be acceptable will be influenced by the availability of resources, the benefit of the protected asset to society and other priorities. The required security measures may take advantage of measures established for radiological safety purposes.

2.50. The regulatory body should develop requirements by using a graded approach applying the principles of risk management, including the categorization of radioactive material in accordance with its risk level.

Graded approach

2.51. Paragraph 3.23 of Ref. [3] states that "The *regulatory body* should develop requirements by using a *graded approach* applying the principles of risk management including a categorization of *radioactive material*."

2.52. Security based categorization when applied to the security of radioactive material in transport refers to the process of categorizing radioactive material based on its activity level and use, assigning an appropriate transport security level and making adjustments to the transport security level and resulting security measures based on specific factors or considerations. Considerations used in the categorization (described in more detail in Section 3) should include the level of threat and the relative attractiveness of the material.

2.53. Requirements based on a graded approach will vary in their depth and rigour commensurate with the threat and the potential radiological consequences resulting from a malicious act involving the radioactive material being protected.

2.54. In addition to using the concept of the graded approach for specifying requirements for security of radioactive material in transport, a State should consider the use of this concept to define security levels for other security measures associated with the transport of radioactive material, including those addressing information protection and trustworthiness of individuals.

Defence in depth

2.55. The regulatory body should require that a defence in depth approach[2] be incorporated into the design of the transport security system to provide the functions of detection, delay and response. This involves implementing a designed combination of successive layers of security equipment, procedures and administrative measures (e.g. the organization of guards and the performance of their duties) and features of the transport equipment (e.g. the conveyance, packages and any protective overpacks).

2.56. When appropriate, the security functions of detection, delay and response should be provided by multiple independent measures so that failure of one measure does not mean loss of a function. For example, detection might rely on observation by personnel and also use electronic measures to detect intrusion into the cargo compartment, and delay might be achieved through multiple independent physical barriers such as the conveyance enclosure, protective overpacks and the package itself.

Methods for specifying risk informed security provisions

2.57. Once the State has completed the national threat assessment, and generated a design basis threat or an alternative threat statement, if desired, the specification of risk informed transport security measure for radioactive materials will involve the following:

(a) Evaluating the potential consequences of malicious acts involving radioactive material;
(b) Establishing transport security levels to be applied to packages or conveyances of radioactive material (discussed in more detail in Sections 3 and 4);
(c) Defining security goals for each transport security level (discussed in more detail in Sections 3 and 4);
(d) Specifying administrative and technical requirements or specific security measures for each security level.

2.58. The stringency of transport security requirements could vary based on threat, risk and the feasibility and cost of implementation of particular sets of requirements. For example, the regulatory body might choose to specify more

[2] Defence in depth is the "combination of multiple layers of systems and measures that have to be overcome or circumvented before nuclear security is compromised" [3].

stringent security measures for shipments of Category 1 radioactive sources as compared to Category 2 radioactive sources, requiring the following for Category 1 sources:

(a) Electronic position monitoring of conveyances;
(b) Additional crew members;
(c) Guards and/or law enforcement personnel;
(d) Escort vehicles;
(e) Redundant communication equipment.

Safety and security interface

2.59. A well-coordinated approach between transport safety and security is needed. With respect to the transport of radioactive material, the State should ensure the following:

(a) A balance is maintained between safety and security concerns throughout the nuclear security regime, from the development of the legislative framework to the implementation of safety and security measures;
(b) Regulatory requirements for safety and security are consistent, especially when responsibilities for safety and security are assigned to different competent authorities;
(c) Safety requirements do not compromise security and security requirements do not compromise safety;
(d) Authorities in charge of nuclear safety and of nuclear security coordinate, as applicable;
(e) Safety culture and security culture are both addressed in an integrated management system;
(f) Security measures for radioactive material in transport take into account those measures required for safety and vice versa, during both normal and emergency situations;
(g) Security measures in place during a response to a nuclear security event do not adversely affect the safety of the transport personnel and the public, to the extent possible.

2.60. Some measures required by safety regulations can also improve security. For example, the seals required on all Type A, Type B, Type C and fissile packagings provide evidence that the package has not been opened. In addition, the tie-downs required to secure a package to the conveyance can also be suitable for affixing security equipment such as locks. However, not all tie-downs are suitable for

security purposes, such as those constructed of webbing or other materials that are not resistant to cutting.

2.61. When designing security systems, the potential security benefits of safety features of the packages used to contain the radioactive material should be considered. For example, as the potential radiological consequences associated with the material being transported increase, so does the weight, size and robustness of the package that needs to be used. Robust, heavy packages can provide security benefits by simply using good quality locks to secure key packaging components such as the closure lid or shields that encase the packaging. Robust, heavy packages also increase the difficulty for an adversary to remove or sabotage the shipment.

2.62. Possible conflicts of safety and security measures during transport should also be considered, such as placarding and labelling,[3] route and mode selection, and information management. For example, if a State were to determine, based on an analysis of the threat, to remove (on an exceptional basis) any markings, placarding or labelling placed externally on the package or the vehicle with information on the hazards of the material, compensatory measures should be applied such as escorting personnel who can provide information on the nature and hazards of the material to emergency responders. Solutions to potential conflicts such as these should be assessed and approved by the regulatory bodies responsible for transport safety and security.

SUSTAINING TRANSPORT SECURITY

2.63. Sustaining the State's nuclear security regime is necessary to ensure it remains effective in the long term. It is advisable to establish a programme for sustainability. Sustainability measures include those applicable to security culture, quality management and information security [27]. Each of these topics is addressed in the sections to follow.

[3] It is important for safety that packagings be clearly labelled and transport vehicles clearly placarded as hazardous, so as to reduce the likelihood of an error during emergency response owing to a lack of information about the contents. However, this placarding and labelling would also provide a potential adversary with information that could assist the adversary in performing a malicious act.

Security culture

2.64. Nuclear security culture plays an important role in maintaining personnel vigilance and sustaining security measures used to protect against sabotage or unauthorized removal of radioactive material during transport. An effective security culture is dependent on effective planning, education, training and awareness, as well as the personnel who plan, operate and maintain the security systems. Even a well-designed security system can be degraded if, for example, the shipper or carrier fails to follow procedures.

2.65. As indicated in IAEA Nuclear Security Series No. 7, Nuclear Security Culture [28], all organizations involved in implementing nuclear security should give due priority to the security culture and to the development and maintenance necessary to ensure its effective implementation in the entire organization.

2.66. Personnel involved in transport operations should be aware of the importance of establishing and maintaining an effective security culture. Such awareness can be achieved by regular briefings on strong and effective security practices and strong adherence to procedures. More detailed guidance on nuclear security culture is available in Ref. [28].

Quality management programme

2.67. The regulatory body should require that shippers, carriers and receivers establish, implement and maintain quality management programmes with the goal of ensuring that security systems are designed, implemented, operated and maintained in a way that meets regulatory requirements for security. In particular, the quality management programme should provide a system for ensuring that all relevant security measures, such as the tracking system and communications equipment, are operating correctly. The quality management programme should apply to all security related activities (technical, procedural and administrative) and should be periodically reviewed. The quality management programme should include the following:

(a) Operating procedures and instructions to personnel (specific to role);
(b) Human resources management and training;
(c) Equipment maintenance, updating, repair and calibration;
(d) Performance testing and monitoring of operating systems;

(e) Configuration management[4] for security systems (including computer systems);
(f) Resource allocation to ensure continued performance of the security system.

2.68. Quality management programmes for safety are influenced by the need for openness and transparency. While the quality management programmes for security will be based on similar concepts, the need to protect the confidentiality of sensitive information will need to be taken into account.

2.69. The quality management programme should comply with International Standards Organization for Standardization documents such as, Quality Management Systems — Requirements (ISO 9001) [29] or, Specification for Security Management Systems for the Supply Chain (ISO 28000) [30]. Certification by an accredited agency could be selected by the regulatory body as a method for meeting the requirements for the quality management system.

Information security

2.70. Access to sensitive information relevant to transport security for radioactive material should be limited to those people who need that information in order to perform their jobs. Key elements of information security include identifying the information that needs to be protected, designating individuals who have authorized access to such information, and protecting such information from disclosure to individuals who do not have this access. Information security measures should be established to ensure confidentiality, integrity and availability (to persons with a need to know the information) of information relating to transport security. In particular, sensitive parts of the transport security plan should be subject to information security measures.

2.71. The regulatory body and other competent authorities should take steps, consistent with national requirements and procedures, to ensure appropriate protection of information relating to transport operations and security systems, the unauthorized disclosure of which could compromise security. This includes identifying which information needs to be protected and the level at which it needs to be protected, using a graded approach.

2.72. The regulatory body should require that shippers, carriers and receivers follow specific provisions for information security.

---

[4] Configuration management helps to ensure that the security system is configured as designed and that any changes are properly designed, verified and implemented.

2.73. Certain information might need to be passed to various recipients for operational purposes (such as ferry bookings and transport network requirements). The stringency of the protection of such information should be proportionate to the risk associated with the unauthorized disclosure of information on such material. However, the protection should not be so stringent that it adversely affects transport operations.

2.74. The State should establish sanctions to be applied for violation of information security requirements. These sanctions should be sufficiently severe to act as a deterrent against such violations and should be commensurate with the risk associated with the unauthorized disclosure of the sensitive information.

2.75. More detailed guidance on security of nuclear information is contained in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [31].

Sustainability management and planning

2.76. Paragraph 3.4 of Ref. [27] states:

> "Managing and planning for sustainable operations at the operational level sustains the nuclear security regime through the continuous allocation of resources for the effective design, operation and maintenance of nuclear security systems and measures."

Shippers, carriers and receivers should engage in sustainability management and planning as appropriate. More detailed guidance on sustainability of nuclear security systems is contained in Ref. [27].

PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

2.77. The State should require that the local authorities, shippers, carriers and all others involved in a shipment are appropriately trained and prepared to respond if a malicious act is undertaken against a shipment of radioactive material. A contingency plan to respond to a nuclear security event occurring during a shipment of radioactive material should be developed by the shipper or carrier and periodic rehearsals, tests or exercises of the plan should be conducted.

2.78. The regulatory body should also require that shippers, carriers, receivers and others engaged in transport security have appropriate and effective security

measures in place to detect nuclear security events and to promptly report and respond to such events.

2.79. The State's regulatory framework should clearly specify the following:

(a) The requirements, roles and responsibilities for contingency planning;
(b) Which contingency response capabilities are to be provided by the State, the operators and relevant stakeholders;
(c) How these capabilities are to be coordinated [17, 18].

2.80. Arrangements should be made to ensure the continued effectiveness of the security system during a nuclear security event.

3. CHARACTERIZATION OF RADIOACTIVE MATERIAL FOR TRANSPORT SECURITY

3.1. Radioactive material should be characterized to determine appropriate security requirements to protect against unauthorized removal or sabotage during transport, in accordance with a graded approach. This characterization should take into account the potential radiological consequences of unauthorized removal or sabotage and subsequent dispersal (e.g. in a radiological dispersal device) or use for other malicious purposes. When multiple radionuclides are transported together (e.g. in the same package or conveyance), the aggregation of material should be considered.

3.2. In some cases, the physical and chemical form of the material might make it particularly attractive to adversaries (e.g. forms that are particularly easy to disperse). This comprehensive approach accounts for different ways the radioactive material might be used or sabotaged in a malicious act.

3.3. In this section, an approach for characterizing radioactive material that is applicable to transport security is provided, including a method for assigning appropriate levels of security. Factors such as radioactive material aggregation, potential radiological consequences of sabotage and attractiveness of radioactive material are also addressed.

RADIOACTIVE MATERIAL CATEGORIZATION

3.4. A categorization system should be established to implement a graded approach to security of radioactive material in transport. Transport security levels should be associated with specific types and quantities of radioactive material defined by the categorization system, thereby identifying when greater levels of protection are warranted. The regulatory body should require that material assigned to higher transport security levels be protected with more stringent security measures during transport than material at lower transport security levels.

3.5. The material to be transported should be characterized to identify the radionuclides, the form and activities of the material in order to assign a transport security level. In some cases, a shipment might consist of a single radionuclide, either in a single package or multiple packages. In other cases, there might be multiple radionuclides within a single package or multiple packages containing multiple radionuclides within a single shipment. The identity and activity level of each of the radionuclides should be identified or if not possible (e.g. for radioactive waste), the identity and activity level of the dominant radionuclides (number of A_2, described in para. 3.8) should be identified.

3.6. The international dangerous goods transport regulations [5] use two categories of material for application of security requirements: all dangerous goods and high consequence dangerous goods. Since radioactive material is a class of dangerous goods, consistency with the dangerous goods regulations can facilitate its transport by minimizing unnecessary complications. Therefore, two categories of radioactive material should be used for the application of security measures to correspond to the two categories in the international dangerous goods transport regulations.

3.7. These two categories, referred to in this publication as transport security levels, can be established using an activity threshold to separate them by security significance. The application of this threshold separates radioactive material into two categories: material with activities below the threshold and material with activities above the threshold. Radioactive material with activities lower than the threshold is assigned to the basic security level and radioactive material with activities equal to or higher than the threshold is assigned to the enhanced security level.

3.8. Depending on the radionuclide, this threshold should be based on the D value or the A value for the particular radionuclide. Paragraph 201 of Ref. [14] states:

> "A_1 shall mean the activity value of *special form radioactive material* that is listed in Table 2 or derived in Section IV and is used to determine the activity limits for the requirements of these Regulations. A_2 shall mean the activity value of *radioactive material*, other than *special form radioactive material*, that is listed in Table 2 or derived in Section IV and is used to determine the activity limits for the requirements of these Regulations."

IAEA Safety Standards Series No. RS-G-1.9, Categorization of Radioactive Sources [32] provides a categorization system based on a set of D values defining the activities of a number of common radionuclides that correspond to the "quantity of radioactive material, which, if uncontrolled, could result in the death of an exposed individual or a permanent injury that decreases that person's quality of life" [22][5].

3.9. Relevant D values can be found in annex I of Ref. [22] for a number of commonly used radionuclides. This list is reproduced in Appendix I of this publication. For the radionuclides listed, the D value should be used in establishing the threshold between sources that should be protected at a basic security level and those that should be protected at an enhanced security level. Further guidance on D values can be found in table 2 of Ref. [32] and in table 1 of Ref. [33].

3.10. All commonly transported radionuclides are assigned A values in Ref. [14]. These values represent the maximum activity that can be safely transported in a Type A or non-accident resistant package. There are two A values listed in Ref. [14], A_1 and A_2, for different forms of material. The A_2 value should be used for security purposes in establishing the threshold for radionuclides not listed in annex I of Ref. [22].

[5] The D value corresponds to the threshold activity of a quantity of radioactive material above which a source is considered to be Category 3 or greater, while an activity of 10D and 1000D represent the threshold activities for quantities of material considered to be Category 2 or greater, and Category 1, respectively.

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. [22], 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.

Appendix I provides the basis for this system.

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.

3.13. For radioactive material transported in excepted packages and for low specific activity (LSA-I) and surface contaminated objects (SCO-I) (see Ref. [14] for further information), 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.

3.14. Such material includes the following:

(a) UN 2908 RADIOACTIVE MATERIAL, EXCEPTED PACKAGE – EMPTY PACKAGING;
(b) UN 2909 RADIOACTIVE MATERIAL, EXCEPTED PACKAGE – ARTICLES MANUFACTURED FROM NATURAL URANIUM or DEPLETED URANIUM or NATURAL THORIUM;
(c) UN 2910 RADIOACTIVE MATERIAL, EXCEPTED PACKAGE – LIMITED QUANTITY OF MATERIAL[7];
(d) UN 2911 RADIOACTIVE MATERIAL, EXCEPTED PACKAGE – INSTRUMENTS OR ARTICLES[8];
(e) UN 2912 RADIOACTIVE MATERIAL, LOW SPECIFIC ACTIVITY (LSA-I), non-fissile or fissile-excepted;

---

[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. Further detailed guidance can be found in Ref. [34].

[7] $10^{-3}A_2$ or less per package, see para. 422 of Ref. [14].

[8] A_2 or less per package, see para. 422 of Ref. [14].

(f) UN 2913 RADIOACTIVE MATERIAL, SURFACE CONTAMINATED OBJECTS (SCO-I or SCO-II), non-fissile or fissile-excepted;
(g) UN 3507, URANIUM HEXAFLUORIDE, RADIOACTIVE MATERIAL, EXCEPTED PACKAGE, less than 0.1 kg per package, non-fissile or fissile-excepted.

ASSIGNING TRANSPORT SECURITY LEVELS

3.15. Once radioactive material has been categorized as above or below the applicable threshold, it should be assigned to a transport security level.

3.16. The State should determine an appropriate basis for categorization of radioactive material for assignment of a transport security level for domestic and international transport. Categorization can be performed on a per package, per consignment or per conveyance basis.

3.17. The per package approach for specifying the transport security level is the simplest approach to apply, but does not take into account the possibility of multiple packages being transported together. There are operational benefits to this approach, such as not requiring carriers to keep a tally of the total activity on the conveyance. However, it might not provide an accurate measure of the potential harm that a single diverted conveyance could result in, as multiple packages could be present on a single conveyance.

3.18. The per consignment approach specifies the transport security level based on the activity of all packages presented for transport by a shipper at one time to a carrier, but does not take into account the possibility of multiple consignments from multiple shippers being carried on a single conveyance. A consignment consists of the package(s) presented for transport by a shipper at one time to a carrier. This approach results in aggregating the total activity offered by a shipper at one time and does not require the carrier to keep a tally of the total activity on the conveyance. However, multiple consignments from multiple shippers could still be accepted by the carrier, which could result in the conveyance being assigned a lower transport security level than that warranted by the aggregate activity of the packages in the conveyance.

3.19. The per conveyance approach provides the best measure of security significance, because all the packages on a conveyance could be seized in a single action by an adversary. However, this approach is very difficult to apply to international air and sea transport where consignments from various shippers

might be consolidated and carriers might not accept the shipment owing to the complexity of keeping track of activity on-board a conveyance when this basis for categorization is applied.

3.20. The per package approach is used in this publication for specifying the transport security level. States might wish to consider either the per conveyance or per consignment approach for domestic transport by vehicle, but a per package approach is recommended for international transport by all modes. When organizing an international shipment, an operator should take into account the domestic approaches chosen by the States involved.

Assignment of transport security levels on a per package basis

3.21. Packages with activity levels lower than the threshold value discussed in the previous section should be assigned to the basic transport security level.

3.22. Packages with activity levels equal to or higher than this threshold value should be assigned to the enhanced transport security level.

3.23. Some packages assigned to the enhanced transport security level might contain very high activity material, in some cases up to several hundred thousand times the D values. Because of the wide range of activity in the enhanced transport security level (ranging from 10D to several hundred thousand D), States might wish to establish subcategories within the enhanced transport security level and specify security measures for each subcategory. For example, the regulatory body could require that packages with between 10D to 1000D be protected using a specified set of security measures and packages with more than 1000D be protected using a more stringent set of security measures.

3.24. In contrast, some material and objects assigned to the enhanced transport security level might present sufficiently limited potential for use in a malicious act that they can be assigned to the basic transport security level. This is possible if the material or objects have either radiological or physical properties that severely limit their effectiveness if used in a malicious act. This can be due to the material or objects being any of the following:

(a) Low specific activity material;
(b) Large contaminated objects (e.g. contaminated packagings);
(c) Activated metals.

3.25. The State could consider assigning materials and objects that it deems to be sufficiently unsuitable for use in a malicious act to the basic transport security level when transported within the State. The State might consider defining subcategories within the basic security level for domestic transport. These subcategories would take into account material activity and attractiveness to potential adversaries (see paras 3.33 and 3.34), with appropriate security measures assigned to each subcategory based on a graded approach.

RADIOACTIVE MATERIAL AGGREGATION

3.26. In some cases, it is necessary to aggregate radioactive material in order to determine whether or not a package or collection of packages exceeds the activity threshold for assignment to the enhanced transport security level, for example, in cases where at least one of the following applies:

(a) More than one radionuclide is transported in the same package (e.g. a moisture density gauge containing ^{137}Cs and ^{241}Am/Be);
(b) The State requires aggregation of packages for domestic transport.

3.27. In such cases, whether or not a package or collection of packages should be assigned to the enhanced transport security level can be calculated by first dividing the activity threshold for categorization of radioactive material of each radionuclide by its activity and then summing the resulting ratios. If this sum is less than 1, then the activity threshold has not been exceeded. In contrast, if this sum is equal to or greater than 1, then the activity threshold has been exceeded.

3.28. This calculation corresponds to the formula:

$$\sum_i \frac{A_i}{T_i} < 1$$

where

A_i is activity of radionuclide i that is present (TBq);

and T_i is transport security threshold for radionuclide i (TBq).

POTENTIAL RADIOLOGICAL CONSEQUENCES OF SABOTAGE

3.29. Nuclear security systems designed to protect radioactive material from unauthorized removal generally also provide some degree of protection for the radioactive material against sabotage [3].

3.30. In some cases, specific security measures to protect against sabotage might be warranted based on the potential of the radioactive material to lead to unacceptable radiological consequences if sabotage occurs.

3.31. The State should identify which shipments warrant protection against sabotage. States might reach different conclusions regarding the types of potential situations that constitute unacceptable radiological consequences. Factors that should be considered include the following:

(a) Package contents (radionuclides, activities, physical and chemical forms);
(b) Package and conveyance design;
(c) Effect of the postulated sabotage event(s) on the contents/package/conveyance combination;
(d) Location where the act of sabotage could occur (e.g. in a highly populated area) [21].

3.32. For additional guidance on determining what constitutes unacceptable radiological consequences see paras 3.93–3.95 of Ref. [25].

ATTRACTIVENESS OF RADIOACTIVE MATERIAL IN TRANSPORT

3.33. The State might wish to adjust the transport security level or specify more stringent security measures for shipments of material that the State determines are particularly attractive to potential adversaries.

3.34. Factors influencing the attractiveness of radioactive material to potential adversaries should be considered, particularly factors that would affect the potential radiological consequences of a malicious act. Such factors include chemical and physical form (e.g. solubility or powder), type of radiation emitted (alpha, beta, gamma, neutron), respirability and the half-life of the radionuclides.

4. ESTABLISHING A REGULATORY PROGRAMME FOR TRANSPORT SECURITY

4.1. This section contains guidance for regulatory bodies on developing or enhancing their regulatory programmes to address the security of radioactive material during transport.

SPECIFYING AND APPLYING TRANSPORT SECURITY REQUIREMENTS

4.2. Paragraph 4.6 of Ref. [3] states that "[t]he *regulatory body* should establish goals or objectives that define the required outcome of *nuclear security systems* for each security level."

4.3. 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.

The prescriptive approach

4.4. In a prescriptive approach, the regulatory body establishes a set of specific security measures that the shipper, carrier and receiver are required to implement. Section 5 provides a set of potential prescriptive security measures.

4.5. Advantages of a prescriptive approach include the following:

(a) Simplicity of implementation for the regulatory body and the shipper, carrier, receiver and others engaged in the transport of radioactive material;

(b) Elimination of the need to transmit sensitive threat information;
(c) Ease of inspection and auditing.

4.6. The use of a prescriptive approach might be particularly appropriate in cases where both the threat and potential unacceptable radiological consequences are low.

4.7. The disadvantage of the prescriptive approach is its relative lack of flexibility. In addition, this approach might not allow the shipper and carrier to optimize security measures.

The performance based approach

4.8. In a performance based approach, the regulatory body defines security goals on the basis of a national assessment of the threat and requires that the shipper and carrier design and implement a combination of security measures to meet these goals. This approach allows for flexibility in choosing the particular security measures to be implemented.

4.9. The advantage of this approach is that it recognizes that an effective transport security system might be composed of many combinations of security measures, and that each shipper's and carrier's circumstances might be unique. The performance based approach is also the most cost effective approach when the necessary knowledge and skills are available.

4.10. The disadvantages of this approach are that it depends upon the security system designer and the regulatory body having sufficient personnel with relatively high levels of security expertise, and on the regulatory body sharing sensitive threat information that needs to be protected by those that receive it.

The combined approach

4.11. In a combined approach, elements are drawn from both the prescriptive and performance based approaches. There are many versions of a combined approach. Three examples are described in the following:

(a) The regulatory body could require the use of a performance based approach for the radioactive material having higher potential consequences, while allowing the application of a prescriptive approach for lower consequence material.

(b) The regulatory body could require that a set of prescriptive requirements be supplemented by using the performance based approach to address particular matters, such as an increase in threat.
(c) The regulatory body could adopt a set of alternative security measures from which the security system designer might choose. The security system designer should then demonstrate that its resulting transport security system, as a whole, meets the applicable security goals.

4.12. The main advantage of the combined approach is that it provides flexibility. It can add a smaller burden on both the State's regulatory body and the shipper, carrier, receiver and others engaged in the transport of radioactive material, since it can utilize provisions from the prescriptive approach as a baseline, with adjustments as necessary to counter the threat.

Process for applying the selected approach

4.13. Figure 1 shows a process a State could follow when deciding which approach to use. The figure highlights the decisions that need to be made by the competent authorities regarding which approach to use, and if the combined approach is chosen, the decisions on which approach is to be used for each transport security level.

FUNCTIONS OF A TRANSPORT SECURITY SYSTEM

4.14. The transport security system should be designed to deter an adversary and to prevent the adversary from completing a malicious act through implementation of security measures that fulfil the three security functions of detection, delay and response. The security system should also include security management measures that provide for the integration of personnel, procedures and equipment.

4.15. Paragraph 4.30 of Ref. [3] states:

> "The transport security system should be designed to take into account the:
>
> — Quantity and the physical/chemical form of the *radioactive material*;
> — Mode(s) of transport;
> — Package(s) being used."

4.16. When visible to a potential adversary, security measures used to implement each security function might provide deterrence, for example, security measures built into the conveyance such as guards, a robust package and padlocks.

4.17. In the context of this publication, the three security functions of detection, delay and response are used to design the transport security system for radioactive material. These measures should be implemented in accordance with a graded approach and considered in the context of the threat assessment.

Detection

4.18. Activities intended to detect unauthorized removal and sabotage should start before the radioactive material is placed in the conveyance, and should continue until the shipment has been completed. For example, inspections of vehicles

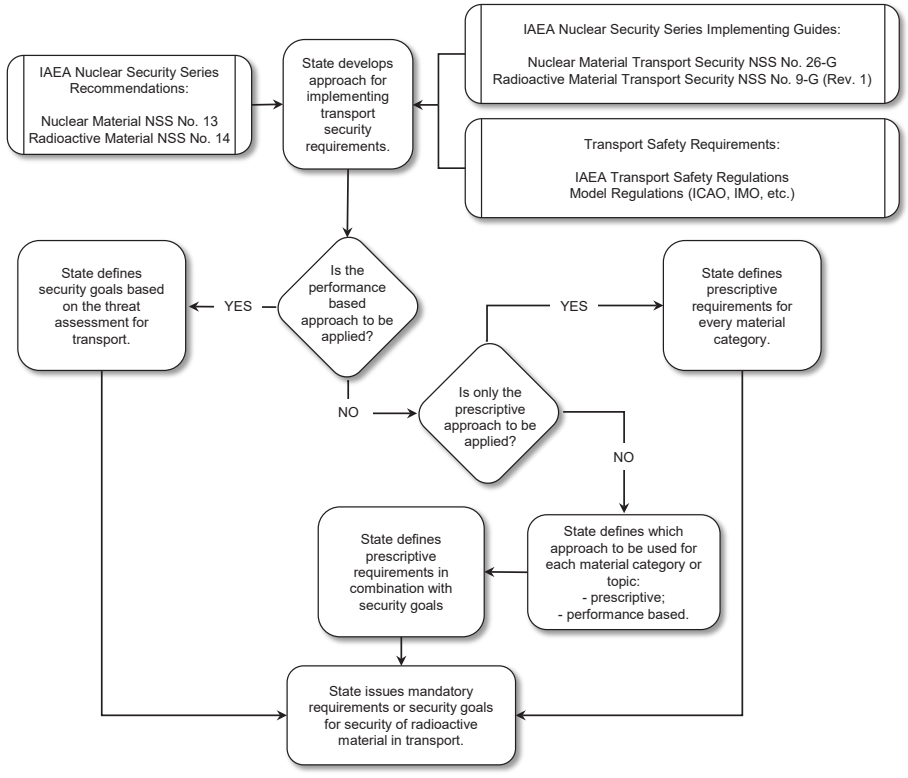


FIG. 1. Decision process for determining the regulatory approach to transport security. ICAO: International Civil Aviation Organization; IMO: International Maritime Organization.

before loading packages can help ensure that the vehicle has not been tampered with and nothing has been affixed to the vehicle that might compromise security.

4.19. Continuous surveillance is frequently used for detection of potential malicious acts. For example, the conveyance crew and the guards involved in the shipment can provide continuous surveillance of the transport conveyance and the surrounding area.

4.20. Technical measures may also be used for detection, such as electronic sensors, video surveillance, audio surveillance, tracking devices, shipment monitoring and duress notification devices (e.g. for drivers and escort personnel).

4.21. Information received from detection alarms, initial observations and other sources should always be rapidly assessed to determine the cause and summon response, if needed.

4.22. In implementing a graded approach, the goal of detection could range from immediate detection, assessment and communication of any unauthorized access (during an attempted malicious act) to detection of unauthorized removal through tamper indicators or verification during transfers and when unloading.

Delay

4.23. Delay measures for transport security are used in order to increase the time needed to remove the material from the conveyance, to provide sufficient time for effective response activities. Delay is considered to be the length of time, after detection, that is needed by an adversary to remove or sabotage the radioactive material. Delay measures include locked doors, overpacks, cages and locking tie-downs, as well as measures such as properly equipped and trained guards.

4.24. In implementing a graded approach, the goals of delay measures could range from providing sufficient delay after detection to allow response personnel to interrupt a malicious act in progress, to providing sufficient delay to assist in timely pursuit of the adversary following an unauthorized removal.

Response

4.25. Response measures should be implemented following detection of a potential nuclear security event and verification that a nuclear security event is underway. The regulatory body should require the shipper, carrier, receiver and others involved with the shipment to make appropriate arrangements for

communicating with law enforcement personnel following the verification of a nuclear security event.

4.26. The response to a nuclear security event can be provided by crew members, accompanying guards or local or regional authorities such as law enforcement. Response measures should have the goal of interrupting a malicious act that is underway and should be capable of preventing completion of the act.

Security management

4.27. Security management addresses the establishment and implementation of policies, plans and procedures for the security of radioactive material in transport as well as the deployment of the necessary resources. Security management includes measures for access control (e.g. to the cargo area, loading and unloading areas and crew areas of the conveyance), trustworthiness verification, information protection, preparation of the transport security plan, training and qualification of personnel and reporting of nuclear security events.

4.28. For shipments assigned to the enhanced transport security level, the regulatory body should require a transport security plan for all entities with security responsibilities relevant to a shipment. The transport security plan formally documents the responsibilities, procedures, arrangements and security systems that will be used.

4.29. The State should establish clear responsibility for the successful development and execution of the transport security plan. The licensee or otherwise authorized organization should hold the responsibility for the security of the material in transport. The responsibility will normally then be assigned by contract to the shipper or carrier that has direct responsibility for the security of the radioactive material. If certain services (e.g. tracking, communications, escort) are subcontracted, arrangements should exist for the subcontractor to comply with the transport security plan.

ESTABLISHING GRADED SECURITY AND CORRESPONDING GOALS

4.30. Paragraph 4.26 of Ref. [3] states that: "Security requirements for *radioactive material* in transport should be developed by the State to minimize the likelihood of loss of control, or *malicious acts*."

4.31. Radioactive material has a wide range of characteristics that make it attractive in varying degrees for use in a malicious act. Some material will be more attractive to an adversary, and other material will be less attractive. The stringency of security requirements should vary with the threat and transport security level. Such an approach takes into account the potential radiological consequences of the radioactive contents. The shipper, carrier and receiver should therefore use a graded approach to implement security measures to ensure that the material is adequately protected.

4.32. To meet the applicable security goal established by the regulatory body for a given transport security level, operators, shippers and receivers should implement security measures to perform the security functions of detection, delay and response, as well as for deterrence and security management.[9] The desired outcome from the combination of security measures implemented to perform each function can be expressed as a set of sub-goals for that function. Sub-goals can also be established for security management.

4.33. Security goals for each transport security level and associated sub-goals are summarized in Fig. 2. Where a sub-goal is shown in the table as the same for two or more columns, it is intended that the sub-goal be met in a more rigorous manner whenever higher confidence is needed that the security system will prevent unauthorized removal.

4.34. Malicious acts can involve either unauthorized removal or sabotage. While the security goals described in Fig. 2 only address unauthorized removal, security systems that achieve the goals can provide some capability to detect, delay and respond to an act of sabotage.

4.35. The regulatory body should require one of the following:

(a) For a performance based approach, that the shipper and carrier demonstrate that the security measures used will meet the applicable security sub-goals.
(b) For a prescriptive based approach, that a set of specific security measures are in place. The regulatory body should ensure that the required measures provide a satisfactory level of security, taking into consideration its assessment of the threat. Additionally, some evaluation of the effectiveness of the measures might be needed (e.g. quality of locks and reliability of communications).

---

[9] Deterrence achieved by a security system is difficult to measure. Consequently, it has not been assigned a set of goals and measures in this publication.

Security goals			
Security functions	Basic transport security level	Enhanced transport security level	Additional security measures
	Confidence that the security system will prevent unauthorized removal	High level of confidence that the security system will prevent unauthorized removal	Very high level of confidence that the security system will prevent unauthorized removal

Security sub-goals			
	Basic transport security level	Enhanced transport security level	Additional security measures
Detection (including assessment)		Provide immediate detection of any unauthorized access to the package	
	Provide detection of any unauthorized removal of the package	Provide detection of any attempted unauthorized removal of the package	Provide immediate detection of any attempted unauthorized removal of the package
		Provide immediate assessment of the detection	
	Verify package count and seal integrity upon delivery		
Delay		Provide delay that the security system will likely prevent the unauthorized removal	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal
Response	Notify authorities	Provide immediate communication to response personnel and notify authorities	
	Implement appropriate action in the event of unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorize d removal
Security Management	Provide written instructions	Provide a transport security plan	
	Ensure trustworthiness and reliability of authorized individuals (e.g. through background checks)		Consider national security clearance approvals as appropriate
	Provide security awareness training	Ensure training and qualification of individuals with security responsibilities	
	Identify and protect sensitive information		
	Provide adequate budget and resources, including a maintenance programme		
	Conduct evaluation for compliance	Conduct evaluation for compliance and effectiveness, including performance testing, exercises and drills	
	Ensure capability to respond to security events	Ensure capability to manage security event covered by the contingency plan	
	Establish security event reporting capability		

FIG. 2. A graded approach for transport security.

5. SECURITY MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF RADIOACTIVE MATERIAL IN TRANSPORT

5.1. This section provides guidance on the content of regulatory requirements to address the security of radioactive material in transport. The regulatory body should satisfy itself that this guidance is incorporated in its regulatory requirements or that another approach has been taken in order to meet the intent of the guidance.

MODE INDEPENDENT PROVISIONS

5.2. States may select a prescriptive approach, in which the regulatory body directly specifies the security measures that the shipper, carrier and receiver should implement to meet the required goals. This might be preferred, for instance, for States where the information and resources needed for the application of a comprehensive methodology for threat assessment and vulnerability assessment, or for the establishment of a design basis threat, are not available.

5.3. Prior to transporting radioactive material, the shipper, carrier and receiver should ensure that all the necessary permits and authorizations for the shipment to proceed have been obtained. If also responsible for security, the shipper, carrier and receiver should ensure that all measures and arrangements for security of the shipment are in place. Appendix II provides additional information on security verifications that should occur prior to transport.

5.4. The remainder of this section provides information on specific security measures that could be used to protect radioactive material against unauthorized removal or sabotage in transport.

Prudent management practices

5.5. Some packages and types of radioactive material are identified in Section 3 as requiring no further security measures other than basic control measures and normal commercial practices. These practices include actions by shippers, carriers and receivers to protect the material against unauthorized removal or sabotage, as would be the case for any valuable commodity.

5.6. Examples of prudent management practices include the following:

(a) Securing and storing the package while in transport (e.g. in a locked conveyance or storage area);
(b) Utilizing carriers with package tracking systems (e.g. bar code system to monitor the status of the shipment), as appropriate;
(c) Using closed vehicles;
(d) Not leaving packages or conveyances unattended for any longer than is absolutely necessary;
(e) Providing drivers of road conveyances with effective communication capability.

5.7. Radioactive material should also be shipped in accordance with all applicable dangerous goods regulations. These requirements will apply for classification, packaging, shipping papers, marking and labelling. These requirements help to bring the attention to shippers, carriers and receiver personnel of the need to handle and transport the packages with due care and diligence.

Basic transport security level

5.8. The guidance in this subsection applies to all packages of radioactive material assigned to the basic transport security level, as discussed in Section 3. For packages assigned to the basic transport security level, prudent management practices, described in the previous subsection, should also apply.

5.9. At the basic transport security level, the regulatory body should require that shippers, carriers, receivers and others engaged in the transport of radioactive material implement security systems or other arrangements to deter, detect, delay and respond to malicious acts affecting the conveyance or its cargo, using a graded approach. These arrangements should be operational and effective at all times and include training and regular briefings to assist personnel in maintaining awareness and vigilance.

Evaluation and exchange of security related information

5.10. Shippers, carriers, receivers and others engaged in the transport of radioactive material should take into consideration all available threat information, including threat information provided by the regulatory body, when implementing security measures.

Protection and control of security related information

5.11. Appropriate measures should be taken to protect sensitive information relating to transport operations, such as information on the schedule and route.

Trustworthiness determination

5.12. A trustworthiness determination[10] is a determination of the reliability of an individual, including characteristics and details that can be verified by means of background checks, where legally permitted and where necessary. Trustworthiness determination is an important element in addressing and controlling insider threats [26].

5.13. The shipper, carrier or receiver should determine the trustworthiness of their personnel who are engaged in the transport of radioactive material. The trustworthiness determination should be based on background checks and used to verify the character and reputation of the individual. For shipper and receiver personnel, the trustworthiness determination might be the same as that required for facility access control. The stringency of this determination should be commensurate with the responsibilities of the individual.

Written instructions, procedures and plans

5.14. Carriers should provide crew members, as appropriate, with written procedures on security measures required by the regulatory body. These procedures should include information addressing how to respond to a security incident during transport. At the basic transport security level, it is generally sufficient for these written procedures to contain no more than details of emergency contacts.

Security training

5.15. Individuals engaged in the transport of radioactive material should receive security training, including basic security awareness training. This training should include training on the need for transport security, the nature of security related threats, methods to address security concerns and actions to be undertaken if a nuclear security event occurs. It should also include awareness of transport

[10] National laws might restrict the scope or conduct of identity verification and trustworthiness assessments in a State. The provisions of this Implementing Guide are without prejudice to the legal rights of individuals, including the right to due process, under national and/or international law.

security plans when appropriate, commensurate with the responsibilities of individuals and their roles in implementing transport security plans.

5.16. Such training should be provided or verified upon employment for all employees involved in the transport of radioactive material and should be periodically supplemented by retraining as deemed appropriate by the regulatory body.

5.17. Records of all security training undertaken should be kept by the employer and should be made available to the employee or regulatory body upon request. Records should be kept by the employer for a period of time established by the regulatory body.

Shipper and carrier credentials

5.18. Each crew member of any conveyance transporting radioactive material should carry means of positive identification during transport, such as an officially issued photographic identification that uniquely identifies the individual.

Receiver and carrier authorization

5.19. Radioactive material should be transported only by registered or authorized carriers and only registered or transferred to authorized carriers and receivers. In those countries where it is not mandatory to be registered or authorized to carry radioactive material, the shipper should verify the suitability and ability of a potential carrier or receiver to transport or receive radioactive material by confirmation with relevant national regulatory authorities or with trade and industry associations, to ensure that the carrier's or receiver's interests are legitimate.

Communications

5.20. During transport, the carrier should provide the capability for crew members to communicate with their company or law enforcement in order to request assistance. This can be done, for example, by using mobile telephones. Communication should remain effective throughout the entire journey. Where this is not possible, predefined communication points in the journey should be agreed to in order to provide evidence that the journey is proceeding as planned without incident.

Open, closed and special conveyance considerations

5.21. Unless there are overriding safety or operational considerations, packages containing radioactive material should be carried in secure and closed or sheeted conveyances, compartments or freight containers. However, packages weighing more than 2000 kg that are locked and secured to the conveyance are appropriate for transport on open vehicles. Whenever it is necessary to use open conveyances, the load should be covered or hidden from view unless precluded by safety requirements. The integrity of the locks and seals used to secure the packages to the conveyance should be verified at all the following stages:

(a) Before dispatch;
(b) Before leaving any stopping point on the route;
(c) On arrival, by staff specifically and previously authorized to undertake this verification.

Conveyance inspections

5.22. Just prior to commencing transport, carriers should perform their own security inspections of the package or conveyance, commensurate with the potential radiological consequences of the material transported, to verify that security measures associated with the conveyance are effective. In normal circumstances and as appropriate to the mode of transport, it is sufficient for the carrier to perform a visual inspection of the package or conveyance to ensure that nothing has been tampered with and that nothing has been affixed to the package or conveyance that might affect the security of the consignment. Such inspections may be performed by transport personnel using their own knowledge of the conveyance or by other security personnel.

Package and conveyance security systems

5.23. The package should incorporate security measures which, while intact, demonstrate that the package has not been opened. Seals required by the transport safety regulations are generally sufficient. The integrity of seals should be verified before dispatch and on arrival. Seals on conveyances and freight containers should also be verified before dispatch and on arrival.

Monitoring and tracking the shipment

5.24. The status of radioactive material in transport should be monitored appropriately. At the basic transport security level, it is sufficient to use a simple

monitoring system such as a package tracking system that can determine when a shipment has departed, when it is in transport and when the consignment has been received. The information about status changes should be readily available to the appropriate parties (e.g. carriers, shippers and receivers).

Continuity of security measures

5.25. If the conveyance makes an expected or unexpected stop, the security measures appropriate for that category of radioactive material in transit should be maintained.

5.26. If left unattended, the conveyance should be secured by locking the vehicle and cargo compartment, as applicable.

5.27. When radioactive material is stored in transit, such as in warehouses and marshalling yards, appropriate security measures should be applied to the material consistent with the measures applied during use and storage. Detailed guidance on security of radioactive material in use and storage is available in Ref. [34].

Receipt verification

5.28. The receiver should have procedures in place to verify package contents, which should include notifying the shipper and carrier if radioactive material is discovered to be missing, or when a package has not been delivered by the expected time.

5.29. The shipper and carrier should have procedures in place to respond to notification from the receiver.

5.30. Through the course of the inquiry, if it is determined that the package or its contents have been lost, stolen or diverted, the shipper and carrier should take action to locate and recover the package or its contents and notify the competent authority as soon as practical.

Enhanced transport security level

5.31. The guidance in this subsection applies to packages of radioactive material assigned to the enhanced transport security level, as discussed in Section 3. For packages assigned to the enhanced transport security level, basic transport security level measures and prudent management practices, described in the previous subsection, should also apply.

Protection and control of security related information

5.32. Measures should be taken to protect sensitive information relating to transport operations, including detailed information on the schedule and route. Such information should be shared on a need-to-know basis, and includes the security system design and operation, response capability, and detection, assessment and delay capabilities. In addition, computer security is critical to protecting sensitive information. Measures should be taken, in accordance with a graded approach, to ensure the security of electronic systems, particularly computer systems.

5.33. More detailed guidance on protection of security related information is provided in Ref. [31].

Written instructions, procedures and plans

5.34. All shippers, carriers, receivers and others engaged in the transport of radioactive material packages assigned to the enhanced transport security level should develop, implement, periodically review as necessary and comply with the relevant provisions of a transport security plan. The regulatory body should require that the licensee develop a transport security plan and might choose to have this plan submitted to the regulatory body.

5.35. The transport security plan should include at least the following elements:

(a) Specific allocation of security responsibilities of organizations and persons engaged in the transport of radioactive material, who have been provided with appropriate authority to perform their responsibilities;
(b) Provisions for keeping records of radioactive material packages or types of radioactive material transported;
(c) Provisions for review of current operations and for vulnerability assessments, including for intermodal transfer, in-transit storage, handling and distribution, as appropriate;
(d) Clear statements of security measures to be implemented that address training, policies, verification of new employees and employment, operating practices, and equipment and resources to be used to reduce security related risks;
(e) Effective procedures and equipment for timely reporting and management of security related threats, breaches of security or security related incidents (e.g. contingency plans);
(f) Procedures for evaluating and testing security plans and procedures for periodic review and update of these plans;

(g) Measures to protect sensitive information;
(h) Measures to ensure that the distribution of sensitive transport information is limited (to maintain security of the information), and measures that do not preclude the provision of transport documents and shipper's declaration as required by the applicable dangerous goods regulations;
(i) Measures to monitor the location of the shipment;
(j) Where appropriate, details concerning agreements on the point of transfer of responsibility for security.

5.36. Shippers and carriers should develop and implement a contingency plan to ensure that there would be an adequate response to malicious acts. This contingency plan could be developed either separately or as part of the transport security plan. If the regulatory body chooses to review the contingency plan, attention should be paid to the adequacy of response force coordination, to ensure an appropriate and timely response to a malicious act.

5.37. Personnel with specific security responsibilities should be provided with written instructions detailing their responsibilities.

5.38. For more detailed information on the content and an example of a transport security plan, see Appendix II.

Shipper and carrier identification

5.39. The regulatory body should identify shippers and carriers engaged in the transport of radioactive material packages assigned to the enhanced transport security level, in order to administer its transport security requirements and to communicate security related information.

Receiver authorization

5.40. Prior to shipping radioactive material, the shipper should verify with the regulatory body that the receiver is authorized to possess the radioactive material.

Planning and coordination

5.41. The shipper, receiver and carrier should agree, prior to transport, on security practices to be followed. Such agreements might be based on normal commercial practices and responsibilities. For example, agreements should exist on the time and place for transfer of the material, such as when and where the shipment is released to the carrier and when and where the shipment is delivered to the receiver.

5.42. The shipper should provide advance notification to the receiver of the planned shipment, mode of transport and expected delivery time. This advance notice should be supplied in time to enable the receiver to make adequate security arrangements for receiving the shipment.

5.43. Prior to commencement of transport, the receiver should confirm the ability and readiness to accept delivery at the expected time and should notify the shipper upon receipt or if the shipment is not received within the expected delivery time frame.

Communications

5.44. During transport, the carrier should provide redundant capabilities for crew members to communicate with contact points specified in the transport security plan.

5.45. When a security related message is transmitted, care should be exercised in the handling of the information to ensure its protection. When open communications are used, techniques such as code words and phrases should be considered.

Open, closed and special conveyance considerations

5.46. Where practical, locks and seals should be applied to conveyances, compartments or freight containers, commensurate with the categorization of the radioactive material being transported. Locks and seals should be checked to confirm the integrity before dispatch, after any stops made during the journey and during any intermodal transfer of each radioactive material consignment. If enclosed freight containers are used, verification of the integrity of a door seal is sufficient, and individual seals on packages inside the freight container do not need to be verified. Lock fittings and components, such as attachment points and tie-downs, should be complementary to the quality and strength of the locks.

5.47. Procedures should be established to ensure the security of keys to conveyances and locks, commensurate with the categorization of the radioactive material being transported.

5.48. Electronic intrusion detection and alarms, including duress alarms, should be considered. Electronic intrusion detection technologies can be suitable for

providing immediate indication of an intrusion into the cargo area. Examples of this technology include the following:

(a) Balanced magnetic door switches;
(b) Light sensors (for closed conveyances);
(c) Fibre optic and other electronic seals;
(d) Passive infrared, microwave or video motion detection.

Monitoring and tracking the shipment

5.49. Automated electronic tracking methods should be used to monitor the movement of conveyances containing radioactive material — for example, using GPS based position tracking of the conveyance — as determined to be appropriate by the regulatory body.

Pre-shipment security verification

5.50. The shipper and carrier should conduct a pre-shipment security verification of the conveyance and security systems prior to commencing transport. The purpose of this verification is to ensure that the security measures are implemented as described in the transport security plan and are functioning normally.

5.51. Pre-shipment security verification should be performed in stages. The first stage (also referred to as 'security arrangement verification') should occur well in advance of shipments, to ensure deficiencies are identified and time is available to resolve them. As an enhanced security measure, final verification just prior to departure (the 'pre-shipment security verification') should also be completed to ensure that all security measures included in the transport security plan are in place and operational. The number and extent of verifications can follow a graded approach, and also be determined based on past history of and experience with earlier shipments.

5.52. Corrective actions should be taken upon identifying that one or more elements are deficient. Without corrective actions, shipments should not be undertaken. Verification checklists can be used to record the need for corrective actions and to document when the corrective actions have been completed.

Additional security measures

5.53. In certain circumstances, the regulatory body might consider requiring additional security measures in view of the current threat level, the design basis

threat or alternative threat statement, or the physical or chemical form and quantity of the radioactive material transported. For example, the regulatory body might require additional security measures for high activity shipments, such as those exceeding 1000D. In such cases, one or more of the following measures should be considered in addition to those identified in paras 5.8–5.52.

Trustworthiness determination

5.54. Consideration might be given to using more stringent trustworthiness procedures to screen personnel with responsibilities for the transport of radioactive material at the enhanced transport security level than required for personnel with responsibilities at the basic transport security level. Such procedures might include national security clearance approvals commensurate with their responsibilities.

Written instructions, procedures and plans

5.55. As stated in the previous section, at the enhanced security level the regulatory body should require that the licensee develop a transport security plan and might choose to have this plan submitted to the regulatory body. The regulatory body might additionally choose to review and approve this plan, including any required additional security measures.

5.56. In addition to the guidance provided in the previous section, exercises can be carried out to ensure that the transport security and contingency plan is adequately evaluated and tested. If the exercises indicate a need for revisions to the transport security and contingency plan, the revisions should be completed and approved by the regulatory body before a shipment is undertaken. Exercises might be limited to arrangements controlled by the shipper and carrier or they might also include State level response arrangements.

Security training

5.57. Additional training might be provided to persons engaged in the transport of radioactive material to ensure that they have the proper skills and knowledge to implement specific security measures associated with their responsibilities.

Shipper and carrier licensing

5.58. Radioactive material carriers might be subject to a regime whereby their operations are licensed and their security programmes are subject to periodic inspection by the regulatory body.

Advance notification

5.59. The regulatory body might require the shipper and carrier to provide advance notification of a shipment to the regulatory body or other competent authorities. Such advance notification might include details of the shipment, including a description of the material being shipped, planned routes, estimated departure and arrival times, and border crossings, as applicable.

Communications

5.60. The regulatory body might consider requiring that a transport control centre or other designated point of communication be established as a central location to monitor and coordinate voice and digital communication.

5.61. Continuous two-way voice communication might be considered between the conveyance, any guards accompanying the shipment, response forces, the transport control centre and, where appropriate, the shipper and receiver.

5.62. The regulatory body might consider requiring that secure communications are used during the transport and that such measures provide redundancy of systems. The use of duress codes and duress button(s) to initiate response might also be considered.

Open, closed and special conveyance considerations

5.63. The regulatory body might consider requiring the use of conveyances that are specially designed or modified to provide additional security features (e.g. a specially designed trailer that allows the package to be secured to the trailer so that the package is not easily removed).

5.64. Vehicle disabling devices might be considered, potentially including the capability to disable the vehicle when parked as well as when it is in motion (controlled shut down).

5.65. In the event that packages need to be transported on open conveyances, it might be necessary for the regulatory body to consider whether additional security measures should be applied, in view of the nature of the radioactive material or prevailing threat. Such measures may include providing guards and enhancing route surveillance or response capability.

Conveyance inspections

5.66. Prior to loading and dispatch, and after any stops, the regulatory body might require that appropriately trained personnel conduct a thorough inspection of the conveyance to ensure that nothing has been affixed to the conveyance and it has not been tampered with in any way that could compromise security.

Monitoring and tracking the shipment

5.67. The regulatory body might consider requiring a transport control centre or other designated point of communication be established as a central location to monitor the shipment, including positional tracking, and to facilitate command and control.

Guards and individuals accompanying the shipment

5.68. The regulatory body might require that guards accompany certain shipments to provide for continuous surveillance of the conveyance. The guards should be adequately trained (especially if they are armed), suitably equipped and fully prepared to fulfil their responsibilities.

5.69. The regulatory body might also require that additional personnel accompany the conveyance in order to maintain surveillance and control during transport and planned or unexpected stops. The additional personnel may be a second driver or crew member.

MODE SPECIFIC PROVISIONS

5.70. In addition to the mode independent provisions mentioned in paras 5.8–5.69, the following provisions should also be considered depending upon the mode or modes of transport to be used in the shipment.

Provisions for road, rail and inland waterway transport

5.71. The shipper and carrier should ensure the application of devices, equipment or other arrangements to deter, detect, delay and respond to theft, sabotage or other malicious acts (including theft of the vehicle or inland waterway craft) affecting the conveyance or its cargo and should ensure that these systems are operational and effective at all times.

Provisions for road transport

5.72. The carrier should maintain continuous attendance of the road conveyance during transport, where possible. Where non-attendance is unavoidable, the road conveyance should be secured and positioned in a well-illuminated area.

5.73. If a road movement cannot be completed without overnight or extended stops, then the radioactive material should be protected during such stops in accordance with a graded approach. Security requirements for radioactive material within a facility might be taken as a basis for defining security requirements to be used for extended stops in transit.

Provisions for rail transport

5.74. If a rail movement cannot be completed without overnight or extended stops, then the radioactive material should be protected during such stops in accordance with a graded approach. Security requirements for radioactive material within a facility might be taken as a basis for defining security requirements to be used for extended stops in transit.

PORTABLE AND MOBILE DEVICES

5.75. The ease of handling and potential for concealing portable and mobile devices[11] can make them vulnerable to unauthorized removal and attractive to potential adversaries.

5.76. For these reasons, specific security measures might be needed in order to take into account their portability. For example, the regulatory body might require that two independent physical barriers be used to secure radiographic devices during transport owing to their ease of portability.

PROTECTION AGAINST SABOTAGE

5.77. As stated in para. 2.1 of Ref. [3], one objective of a State's nuclear security regime applicable to transport of radioactive material should be

[11] Portable and mobile devices refer to pieces of equipment containing radioactive material that can be carried by hand, mounted on wheels or casters, or otherwise moved without the need for disassembly or dismounting.

"Protection against *sabotage* of *other radioactive material*, *associated facilities* and *associated activities*".

5.78. The State should identify the criteria that define what constitutes radiological consequences sufficiently high to warrant protection against sabotage. These criteria might be specified in terms of any of the following:

(a) The quantity of radioactive material calculated to be released as a result of the sabotage event (an activity threshold);
(b) The dose or dose rate at a defined distance from the event location;
(c) Any other quantity the State determines is appropriate.

5.79. An evaluation of the potential for sabotage during transport, and a determination of the associated potential radiological consequences, might be required by the regulatory body. This evaluation should be performed in close consultation with safety specialists since the transport packaging required for safety purposes might also provide significant protection. Protection against sabotage should be implemented with consideration of the measures for safety and the measures against unauthorized removal.

Threat assessment

5.80. The State should assess known and potential threats to radioactive material transport, specifically taking into account the intent and capability of potential adversaries to commit acts of sabotage. For example, an adversary might seek to release radioactive material in sufficient quantities to result in unacceptable radiological consequences. However, even an act of sabotage that is unsuccessful in releasing material might lead to harmful consequences. Additional information on threat assessment, a design basis threat and an alternative threat statement can be found in Ref. [24].

Development of specific threat scenarios

5.81. The design basis threat or alternative threat statement developed by the State should take into account credible scenarios involving sabotage of shipments of radioactive material. Such scenarios should reflect the capabilities of the threat as determined by the State's threat assessment. For example, one aspect of a scenario that might be considered is the size of the adversary force and the training and experience of the adversary. A second aspect is the attack methods that could be used to achieve the sabotage objective.

Target identification and ranking

5.82. From a State's standpoint, potential targets for sabotage could be any radioactive material shipment occurring on the territory of the State or, while in international water or airspace, carried by a ship or aircraft flagged or registered to the State. The State should identify which shipments it believes warrant protection against sabotage owing to the potential for unacceptable radiological consequences.

Estimating the consequences of sabotage considering the threat and the targets

5.83. Potential radiological consequences associated with the sabotage of radioactive material shipments should be estimated, primarily based on the activity of the radionuclide(s) but also taking into account the physical and chemical form of the material.

5.84. Safety features of the package and conveyance as well as measures to prevent unauthorized removal should also be taken into account in estimating the potential radiological consequences of a sabotage attempt. The structure of the conveyance and the radioactive material packaging will provide some protection for the material. The degree of protection provided varies with the material being transported and the robustness of the packaging required for safety purposes.

5.85. An act of sabotage against radioactive material in transport using an explosive device could result in a variety of consequences, including the following:

(a) Damage owing to the blast of the explosive (generally limited to a radius of a few hundred metres);
(b) Dispersion of large particles or pieces of radioactive material (generally limited to a radius of a few hundred metres);
(c) Airborne dispersion of smaller particles, including respirable particles, which can be carried thousands of metres depending on the buoyancy of the plume created by the blast and accompanying fires.

5.86. For any radioactive material, the radiological consequences of sabotage that result in a release of the material could include the following:

(a) Dose due to external exposure to unshielded material that is localized (such as an unshielded sealed source);
(b) Dose due to external exposure to dispersed material;

(c) Dose due to internal exposure from inhaled airborne material that is generated by the event, or material that is suspended after deposition or ingested from food or water contaminated by the release from the sabotage event.

5.87. In the most basic terms, the severity of radiological impact is directly linked to the types and amounts of radiation released to the environment from which people could receive a dose directly or which would prevent normal social and economic activity. Thus, listed below are the two principal determinants of the severity of a radiation release from a shipment subjected to sabotage:

(a) Radionuclide content of the package or shipment;
(b) Fraction of the radioactive contents of the shipment potentially releasable as a result of the sabotage event.

5.88. The State should perform an analysis of the potential radiological consequences of sabotage that could occur during transport of radioactive material. The potential activity release determined by the analysis should be compared to the threshold determined by the State for unacceptable radiological consequences, as discussed in Ref. [3]. If the threshold defined by the State is based on dose or dose rate, this information should be calculated from the potential activity release, taking into account the radionuclides and form of the material released.

5.89. If the calculations show that sabotage could result in radiological consequences that exceed the State's defined threshold for unacceptable radiological consequences, then additional protective measures might be necessary in addition to the measures required by the regulatory body to protect the material against unauthorized removal. The degree to which the potential radiological consequences of sabotage exceed the State's threshold for unacceptable radiological consequences will be one of the principal determinants of the amount of effort undertaken to minimize the potential radiological impacts of a successful sabotage event. The shipment contingency plan should also be reviewed to ensure that it adequately addresses actions to respond to sabotage situations.

5.90. It might also be possible to add some additional protection features to the transport package or its conveyance to limit the projected release to an acceptable value.

Defining security measures for protecting against sabotage

5.91. Paragraph 4.37 of Ref. [3] includes the following recommendation:

> "If the current or potential *threat* warrants additional security measures to protect against *sabotage*, consideration should be given to:
>
> — Postponing the shipment;
> — Rerouting the shipment to avoid high threat areas;
> — Enhancing the robustness of the package or the vehicle;
> — Enhancing route surveillance to observe the current environment;
> — Providing (additional) escorts or guards."

5.92. Paragraph 4.36 of Ref. [3] also recommends that "[w]hen establishing security measures to protect against a *malicious act* particularly *sabotage*, the safety features of the design of the transport package, container and conveyance should be taken into account."

Applicable security measures

5.93. A variety of features could be used with existing packagings to minimize the release of radioactive material to the environment in case of an attack on a shipment. Several of these features also can be used to counter unauthorized removal of the material by increasing the time needed to retrieve the material from the packaging (delay measures).

5.94. Both active and passive measures are possible. For example, measures might include those that protect against an attack device being placed close to the package or conveyance, such as protective metal covers. Conveyances transporting spent fuel casks might be fitted with covers that can reduce the effectiveness of explosives and reduce the penetration abilities of stand-off attacks.

5.95. Most of the measures will result in additional procedures to be used for the preparation of a shipment. The measures taken should not adversely affect the safety of the package.

Applicable organizational measures

5.96. The State should consider the need for compensatory protective measures such as additional guards, barriers and surveillance when packages are removed from their conveyances during loading, unloading and transhipment. Additional

inspections prior to movement can also be made to ensure that nothing has been attached to the package, container or conveyance that could cause damage.

5.97. Operational measures might include changes in the route to avoid highly populated areas where the radiological and economic consequences of a successful sabotage event might be very high.

5.98. If a review of the nuclear security measures implemented to protect a shipment of radioactive material indicates that the measures are not sufficient to counter the current threat of sabotage, the State may consider postponing the shipment.

6. MEASURES TO LOCATE AND RECOVER RADIOACTIVE MATERIAL MISSING OR STOLEN DURING TRANSPORT

STATE RESPONSIBILITIES

6.1. The State should ensure that roles and responsibilities are clearly defined within its regulatory framework for situations where radioactive material is determined to be lost, missing, or stolen during transport. The State should implement the recommendations in Ref. [4]. Procedures should be established to ensure that information and assistance is available to support rapid and comprehensive measures to locate and recover lost, missing or stolen radioactive material.

6.2. Shippers, carriers and receivers should be required to notify the regulatory body within a specified time of any radioactive material that is determined to be lost, missing, or stolen during transport. Once a package with radioactive material has been reported to be lost, missing or stolen during transport, the situation should then be considered to be out of the shipper's or carrier's control.

6.3. The State should ensure that national contingency plans are established for the actions it will take to locate and recover any radioactive material that is reported as lost, missing or stolen during transport. These contingency plans should be coordinated with national emergency response plans [17, 18].

6.4. The carrier should be alert during transport and delivery for any indications that packages have been lost, missing or stolen from the conveyance or that tampering has occurred.

6.5. Upon discovery that a package has been lost, missing or stolen from a conveyance, the carrier should initiate an immediate search to determine if the package might have been inadvertently misplaced, but remains under the carrier's control. If loss of control is confirmed, the carrier should notify the relevant authorities and, as good practice, the shipper. Additionally, the carrier should provide assistance with all efforts to locate the package (i.e. tracing previous movements and handling transactions, and providing requested information) and should fully cooperate during any subsequent investigations and prosecutions.

6.6. Additionally, as good practice, the carrier might wish to notify the competent authority upon suspicion that a package has been lost, missing or stolen, or upon suspicion that a package has been tampered with.

6.7. If the carrier locates a package that has been reported lost or missing after it has notified the shipper and the relevant authorities of an incident, the carrier should promptly inform them that the package has been found.

Appendix I

SETTING THE TRANSPORT SECURITY LEVELS[12]

MALICIOUS USE OF RADIOACTIVE MATERIAL

I.1. The following scenarios represent broad categories of possible malicious acts with the potential to give rise to significant radiological consequences:

(a) Covert placement of unshielded material in working and living areas or street locations where the public might be exposed to radiation.
(b) Sabotage of radioactive material packages or shipments with a subsequent release of radioactive material and its dispersal into the environment.
(c) Capture of a radioactive material package or shipment and the subsequent dispersal of the material by means of conventional explosives.
(d) Capture of a radioactive material package or shipment and its subsequent processing, for example the transformation into a more highly dispersible form, with subsequent dispersal of the radioactive material in the environment (i.e. a radiological dispersal device scenario). The time and resources needed for this action would increase the likelihood of successful intervention by security forces, therefore this scenario is considered less likely than others.

I.2. The radiological consequences arising from attacks of each of these types are extremely variable and depend on, for example, the type and nature of the event and the type and amount of radioactive material involved.

I.3. In a situation, such as para. I.1(c), involving the capture of a radioactive material package or shipment and the subsequent dispersal of the material by means of conventional explosives, the main radiological consequences from such an event (i.e. a radiological dispersal device scenario), include both near field and far field effects. In the vicinity of the explosion (near field), there might be radioactive shrapnel and larger pieces of radioactive material dispersed in the area, injuring persons and damaging and contaminating buildings. General contamination from vaporized or finely divided material might also be present. Persons in the area might inhale vaporized or finely divided material and their skin and clothes might be contaminated. There might also be a rising plume that disperses vaporized and finely divided material (to the far field) resulting in

[12] This appendix is based on Ref. [22].

contamination of the area and of persons in the area, as well as exposure due to inhalation as the plume passes.

I.4. Since the radiological dispersal device scenario might be a very attractive means for adversaries to cause harm and can be undertaken with unsophisticated capabilities, it is considered a more likely scenario. It is appropriate to apply the evaluation of potential radiological consequences of a malicious act involving different radionuclides to the radiological dispersal device scenario.

ESTABLISHING TRANSPORT SECURITY LEVELS

I.5. Because radioactive material is considered to be a dangerous good, and thus its transport occurs within the broader framework of the transport of all dangerous goods, it is desirable to be as consistent as possible with existing security requirements and guidelines, particularly the UN Model Regulations [5] and the international modal regulations [6, 7]. Additionally, it is desirable to be consistent with relevant provisions of the Code of Conduct [22], with its supplementing guidance [23], the Convention on the Physical Protection of Nuclear Material, together with its Amendment [12, 13], and Ref. [2]. The transport security levels included in this publication have been developed with these considerations in mind.

I.6. Since transport operations vary widely in how they are performed (e.g. a single package, consignments of individual packages), a clear basis should be used to specify the transport security level. The following are the three feasible bases for specifying which shipments should be subject to enhanced transport security measures:

(a) *Per package approach*: Enhanced security provisions would be applied when the activity of any package in a consignment exceeds the threshold value;
(b) *Per consignment approach*: Enhanced security provisions would be applied when the activity in a consignment exceeds the threshold value;
(c) *Per conveyance approach*: Enhanced security provisions would be applied when the total activity on a conveyance exceeds the threshold.

I.7. The per package approach is used in this publication for specifying the transport security level. States might consider either the per conveyance or per consignment approach for domestic transport by vehicle, but a per package approach should be used for international transport by all modes.

I.8. There are some packages of radioactive material with such low levels of radioactivity that they present low radiological hazards and correspondingly low security risks (e.g. consumer products, very small quantities of radionuclides and material with very low activity concentration). Because of the very limited potential consequences that could arise from their use in malicious acts, certain packages and materials need not be subjected to transport security provisions more stringent than those ordinarily applied to a commercial shipment. These packages and materials are defined and specified in Ref. [14] and are also identified by their UN number. These packages and materials should meet the following activity limits and other specifications contained in Ref. [14]:

(a) Empty packagings — UN 2908;
(b) Articles manufactured from natural uranium, depleted uranium or thorium — UN 2909;
(c) Excepted packages with an activity level not exceeding the level permitted for the radionuclide when it is not in special form — UN 2910 and UN 2911;
(d) Low specific activity materials (LSA-I) — UN 2912;
(e) Surface contaminated objects (SCO-I) — UN 2913;
(f) Uranium hexafluoride, radioactive material, excepted package, less than 0.1 kg per package, non-fissile or fissile-excepted — UN 3507.

I.9. Normal commercial controls and safety regulations applied to these shipments are appropriate for their very low potential consequences if used in a malicious act.

I.10. For packages and materials exceeding the activity level allowed in those listed in para. I.8, the potential consequences of their use in a malicious act vary greatly. In order to specify appropriate transport security measures, packages might be grouped on the basis of their potential consequences. Having two transport security levels is desirable for simplicity, and introducing transport security sublevels makes it easier to tailor the security measures more precisely to the potential radiological consequences of the material.

I.11. Two transport security levels should be used to specify transport security measures for packages containing a quantity and type of radioactive material that could result in very limited potential consequences. The use of two levels allows the security measures to be specified as simply as possible while separating packages into types that warrant either basic or enhanced security measures.

I.12. The use of these two levels (basic and enhanced) for transport security indicates that a threshold is needed to specify which of the two levels is assigned

to a package. An activity threshold should be used, because the potential radiological consequences associated with the contents of a package depend on the radionuclides and activity levels in the package. The use of a single activity threshold is also consistent with the approach to the transport of dangerous goods of the UN Model Regulations [5]. The threshold used in the UN Model Regulations distinguishes between high consequence radioactive material packages and other radioactive material packages (i.e. above the level of excepted packages, LSA-I and SCO-I, which do not warrant security measures beyond prudent management practices). The term 'high consequence dangerous goods' is used in the UN Model Regulations and corresponds to the use of an enhanced security level in this publication.

I.13. This approach results in the following three transport security levels:

(a) *Prudent management practices:* Consignments consisting of excepted radioactive material packages (with contents not exceeding the activity allowed for the radionuclide(s) in non-special form) and radioactive material specified as LSA-I and SCO-I. No additional provisions other than those control measures required by Ref. [16] and normal commercial practices are suggested.
(b) *Basic transport security level*: Consignments consisting of packages analogous to other dangerous goods subject to the 'general provisions' for dangerous goods security in the UN Model Regulations [5] (packages that are below the specified activity threshold).
(c) *Enhanced transport security level:* Consignments that include at least one package analogous to high consequence dangerous goods as defined in the UN Model Regulations [5] (i.e. a package that is above the activity threshold).

I.14. In certain circumstances, additional security measures might be considered by a State, as discussed in paras 5.53–5.69.

I.15. The transport security levels and the application of progressively more stringent security measures, along with prudent management practices providing the baseline and additional security measures available as needed, are illustrated in Fig. 3. This diagram reiterates that each successive transport security level builds upon the previous level, where more stringent security measures are applied generally as the activity of the radioactive material increases. The activity threshold of 10D or $3000A_2$ separates the basic and enhanced transport security levels. Prudent management practices apply regardless of the radioactive

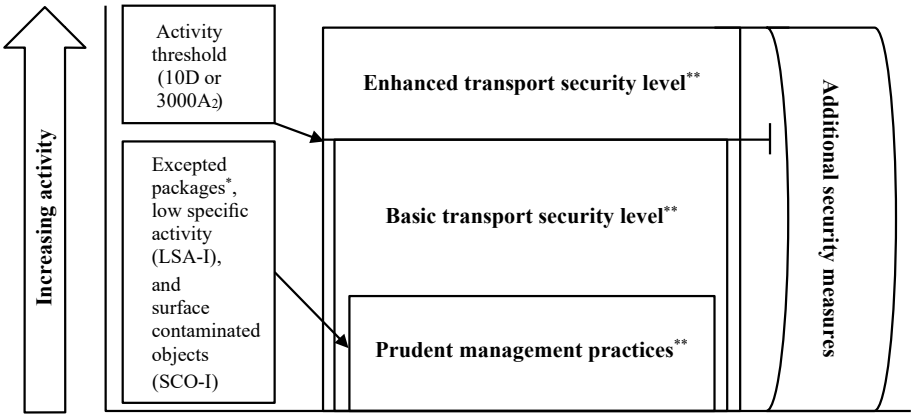
material and additional security measures might be necessary regardless of the security level.

DEFINING THE ACTIVITY THRESHOLD

I.16. To specify which packages should be transported using enhanced security measures, it is necessary to define the activity level that would constitute high consequence radioactive material.

I.17. Considerable work has been done to define a dangerous source, see Refs [32] and [33]. This work identifies exposure scenarios and dose criteria used to define the quantity of a radionuclide which, if uncontrolled, could result in the death of an exposed individual or a permanent injury that decreases that person's quality of life (the D value).

I.18. Recognizing that the Code of Conduct [22] is being implemented by many Member States, the approach embodied in the Code was examined to determine whether it could be used for setting the activity thresholds for the radionuclides included in the Code. Reasonable correlation was found with 1000D for beta/gamma emitters and 10D for alpha emitters. Although sources with an



*Excepted packages with activity not exceeding the level permitted for the radioactive material when it is not in special form (see para. 422 of Ref. [14]).

**The regulatory body may require additional security measures in addition to any security measures already prescribed for a given transport security level.

FIG. 3. Transport security levels.

activity exceeding the D values specified in Refs [22, 32, 33] are considered dangerous (i.e. they could result in the death of an exposed individual or a permanent injury that decreases the person's quality of life) it is not considered realistic to implement enhanced security measures for all sources with an activity exceeding the D values. Considering this, a threshold of 10 times the D values is recommended to specify the enhanced transport security level for radionuclides listed in the Code to include Category 1 and 2 sources [22].

I.19. For radionuclides not included in the Code of Conduct [22], another approach is needed for specifying the activity threshold. A strong desire has been expressed by Member States to specify the activity threshold in terms of the traditional transport safety A values. These values are calculated using the 'Q system' that has been incorporated in the IAEA guidance on transport regulations for over 35 years as described in IAEA Safety Standards Series No. SSG-26, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material [35].

I.20. The A_1 values are derived for special form (non-dispersible) radioactive material and the A_2 values are for other than special form (dispersible) radioactive material. The A values are not based on exposure scenarios that are appropriate for representing the potential consequences of a radiological dispersal device. However, they are derived from transport accident scenarios and well established in relation to the transport of radioactive material. Consequently, a multiple of the A values was considered to be the desired way to express the activity threshold. When the radionuclides covered by the Code of Conduct [22] are disregarded, the remaining radionuclides showed good correlation with a value of $3000A_2$ (since the A_2 value of a radionuclide never exceeds the A_1 value). Subsequently, for radionuclides not included in the Code of Conduct [22], a value of $3000A_2$ may be used to identify packages that are subject to the enhanced transport security measures. This does not mean that $3000A_2$ corresponds to the same risk of causing severe deterministic health effects as 10D.

BASIS FOR THE TRANSPORT SECURITY THRESHOLD

I.21. To facilitate the undertaking of the transport security measures, the following definition of high consequence radioactive material is used:

(a) $3000A_2$ in a single package for all radionuclides not listed in Table 1;
(b) The transport security threshold value corresponds to the radionuclides listed in the Code of Conduct [22], as shown in Table 1.

TABLE 1. TRANSPORT SECURITY THRESHOLD (10D VALUES) FOR RADIONUCLIDES LISTED IN THE CODE OF CONDUCT [22]

Radionuclide	Transport security threshold (TBq)
Am-241	0.6
Au-198	2
Cd-109	200
Cf-252	0.2
Cm-244	0.5
Co-57	7
Co-60	0.3
Cs-137	1
Fe-55	8000
Ge-68	0.7
Gd-153	10
Ir-192	0.8
Ni-63	600
Pd-103	900
Pm-147	400
Po-210	0.6
Pu-238	0.6
Pu-239	0.6

TABLE 1. TRANSPORT SECURITY THRESHOLD (10D VALUES) FOR RADIONUCLIDES LISTED IN THE CODE OF CONDUCT [22] (cont.)

Radionuclide	Transport security threshold (TBq)
Ra-226	0.4
Ru-106	3
Se-75	2
Sr-90	10
Tl-204	200
Tm-170	200
Yb-169	3

I.22. The model used to define suitable thresholds for the enhanced transport security level is based on a combination of 10 times the D values[13] and 3000 times the A_2 values[14]. These values were used to harmonize with the existing international requirements and recommendations, the existing national nuclear security regulations and requirements of many Member States, and with practical consideration of consistency with the Code of Conduct [22].

[13] For radionuclides listed in annex I of the Code of Conduct (see Ref. [22]).
[14] For all other radionuclides not listed in annex I of the Code of Conduct (see Ref. [22]).

Appendix II

TRANSPORT SECURITY PLAN

II.1. The transport security plan describes the security arrangements, personnel and equipment that will be used to provide security during transport. The entities responsible for having a transport security plan are normally the shipper, carrier, receiver and any other entity having direct responsibility for the security of the radioactive material in any particular mode or phase of the transport.

DEVELOPING THE TRANSPORT SECURITY PLAN

II.2. A first step in developing the transport security plan is an evaluation of potential vulnerabilities for the shipment or campaign (i.e. a series of identical or similar shipments) that will be subject to the transport security plan. Such an assessment should take into account all information, as appropriate, with regard to: (a) the mode or modes of transport; (b) intermodal transfers; (c) the route to be followed; (d) any transit sites, stop-over points, temporary storage or transfer areas; (e) conveyances, equipment and personnel; and (f) planned or potential stopping places. The result of this assessment is then used to make a judgment as to whether the overall effectiveness of the security system is adequate or if improvements such as compensatory measures are needed.

II.3. The transport security plan should be designed so that it can be modified as needed to reflect the threat level at the time of use as well as reflect any changes to the transport arrangements. The transport security plan should address routing of the shipment, stopping places, destination hand over arrangements, identification of persons authorized to take delivery, emergency arrangements, contingency plans and reporting procedures (both routine and emergency). The transport security plan may address single or multiple similar shipments and may be valid for a specified period of time. The transport security plan should be protected as sensitive information and should only be discussed with organizations as it applies to their roles and responsibilities (the plan, in its entirety, should not be discussed, unless appropriate). Such sensitive information should not be included in procedures or documents that are developed for other purposes and that may be disseminated more widely. For information security reasons, the transport security plan may be developed in the form of a series of separate documents, each of which may be provided only to those that need to know those parts of the plan.

II.4. All shippers, carriers, receivers and others engaged in the transport of radioactive material should have contingency plans in place to respond to malicious acts involving radioactive material in transport, including plans for actions to take for recovery of lost or stolen material and for mitigating radiological consequences of sabotage. These contingency plans may be a separate document or a part of the transport security plan.

SUBMITTING AND OBTAINING APPROVAL OF THE TRANSPORT SECURITY PLAN

II.5. The regulatory body should specify whether a transport security plan and, if required, any associated vulnerability assessment needs to be submitted to the regulatory body for review and approval. This might depend upon the category of material being proposed for transport. For example, transport security plans could be required for both Category 1 and 2 radioactive material shipments but approval of transport security plans could only be required for Category 1 shipments. The approval process can also be iterative. If the regulatory body feels that the requirements are not met in the proposed transport security plan or that the results of the vulnerability assessment are inadequate, the transport security plan and vulnerability assessment, along with a list of the identified shortcomings, should be returned to the originator for additional information and revision. A scheme for regulatory review and approval of a vulnerability assessment and a transport security plan is provided in Fig. 4.

IMPLEMENTING THE TRANSPORT SECURITY PLAN

II.6. Once the transport security plan has been prepared and, if required, approved by the regulatory body, detailed plans and preparations for the shipment can proceed. Security of the shipment should be provided in accordance with the transport security plan and associated written instructions and agreements.

II.7. After commencing transport, if the shipment cannot be completed in accordance with the transport security plan, the shipper or carrier should immediately implement compensatory measures to maintain the desired level of protection. If the transport security plan has been approved by the regulatory body, the shipper or carrier should inform the regulatory body as soon as practicable. The regulatory body might require the shipper or carrier to prepare a set of compensatory measures in advance.

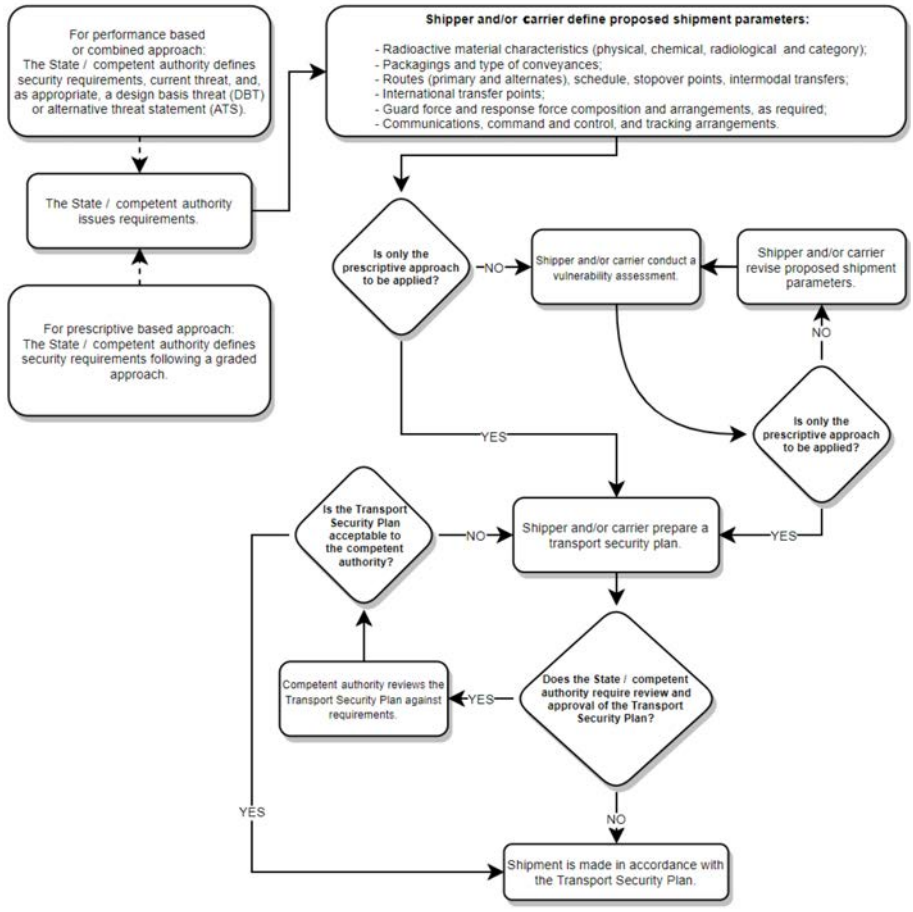


FIG. 4. Sample process for review and approval of a transport security plan by the regulatory body, and a vulnerability assessment, if needed.

II.8. If any incidents or unscheduled delays have occurred during transport, a review of security arrangements should be conducted to evaluate the effectiveness of the transport security plan and to identify any improvements to be made to optimize its effectiveness for future shipments.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

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

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE, Recommendations on the Transport of Dangerous Goods: Model Regulations (Rev. 20), 2 vols, UNECE, New York and Geneva (2017).

[6] INTERNATIONAL MARITIME ORGANIZATION, International Maritime Dangerous Goods (IMDG) Code, IMO, London (2018).

[7] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Technical Instructions for the Safe Transport of Dangerous Goods by Air, ICAO, Montréal (2014).

[8] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE, European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), UNECE, New York and Geneva (2015).

[9] INTERGOVERNMENTAL ORGANIZATION FOR INTERNATIONAL CARRIAGE BY RAIL, Regulations concerning the International Carriage of Dangerous Goods by Rail (RID) (2019).

[10] UNITED NATIONS, European Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterway (ADN), ECE/TRANS/231 (Vol. 1), UN, New York and Geneva (2017).

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material, IAEA International Law Series No. 2, IAEA, Vienna (2006).

[13] Nuclear Security — Measures to Protect Against Nuclear Terrorism: Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10 GC(49)/INF/6, IAEA, Vienna (2005).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, 2018 Edition, IAEA Safety Standards Series No. SSR-6 (Rev. 1), IAEA, Vienna (2018).

[15] 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).

[16] 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).

[17] 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).

[18] 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).

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

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency Involving the Transport of Radioactive Material, IAEA Safety Standards Series No. SSG-65, IAEA, Vienna (in preparation).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on the Import and Export of Radioactive Sources, IAEA/CODEOC/IMO EXP/2012, IAEA, Vienna (2012).
[24] 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 (in preparation).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[29] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Quality Management Systems — Requirements, ISO 9001:2015, ISO, Geneva (2015).
[30] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Specification for Security Management Systems for the Supply Chain, ISO 28000:2007, ISO, Geneva (2007).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (D Values), EPR D VALUES 2006, IAEA, Vienna (2006).
[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).
[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material (2012 Edition), IAEA Safety Standards Series No. SSG-26, IAEA, Vienna (2014). (A revision of this publication is in preparation.)

Annex I

CONTENT AND ORGANIZATION OF THE TRANSPORT SECURITY PLAN

I–1. An example structure of a transport security plan is provided in Box I–1 below. The regulatory body might need to modify this structure to reflect its own particular circumstances, but the example contains the types of information that are typically needed by the regulatory body to validate and approve the proposed security measures and arrangements. The structure of the transport security plan provided aims to facilitate understanding between shippers, carriers, receivers, others involved in the transport, and regulators both domestically and internationally.

I–2. The text in Box I–2 follows the structure from Box I–1 and presents the details to be considered for inclusion in a transport security plan for a shipment of radioactive material.

BOX I–1. EXAMPLE STRUCTURE OF THE TRANSPORT SECURITY PLAN

1. SCOPE
2. OBJECTIVES
3. DESCRIPTION OF THE SHIPMENT AND MATERIAL TO BE TRANSPORTED
   - 3.1. Description of radioactive material
   - 3.2. Mode(s) of transport
4. ADMINISTRATIVE REQUIREMENTS
   - 4.1. Policies and procedures
   - 4.2. Vulnerability and threat assessment
   - 4.3. Testing and evaluating the transport security plan
   - 4.4. Transport security verification
   - 4.5. Notification of relevant agencies
   - 4.6. Review and update of the transport security plan
5. PERSONNEL QUALIFICATIONS
   - 5.1. Trustworthiness
   - 5.2. Training
6. RESPONSIBILITIES
   - 6.1. Organizational structure
   - 6.2. Allocation and transfer of responsibilities
7. INFORMATION MANAGEMENT
   - 7.1. Information security
   - 7.2. Records retention
8. TRANSPORT SECURITY MEASURES
   - 8.1. Routes
   - 8.2. Transport security system
     - 8.2.1. Conveyance
     - 8.2.2. Operations command and control
     - 8.2.3. Nuclear security measures
     - 8.2.4. Communications and positional tracking for normal operations
     - 8.2.5. Maintenance and testing of systems and equipment
9. EMERGENCY RESPONSE
   - 9.1. Emergency and contingency response
   - 9.2. Communications during incidents
   - 9.3. Reporting of threats and incidents

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN

1. SCOPE

This section defines the shipments and entities that are covered in the transport security plan, including the following:

— The type of radioactive material to be shipped;
— The locations of the shipper and receiver;
— The identification of the carrier;
— The regulations and requirements that were used in the development of the transport security plan.

This section includes the complete legal name and address of the entity responsible for preparing and submitting the transport security plan. This includes information about the shipper, carriers, receiver and other entities involved with the shipment, including guards employed for the shipment, and information about transit States when international transport is involved.

2. OBJECTIVES

This section provides a clear statement of the objectives that the plan intends to accomplish, including the following:

— Ensuring security to protect personnel, equipment and radioactive material;
— Providing clear direction to personnel on the following actions to be taken:
  • Ensuring security of shipments;
  • Providing appropriate response to incidents.

3. DESCRIPTION OF THE SHIPMENT AND MATERIAL TO BE TRANSPORTED

3.1. Description of radioactive material

The description of the material to be transported includes the following:

— Nature of the material;
— Type;
— Quantity (activity);
— Physical and chemical characteristics;
— Category;
— Hazards;
— Packaging;
— Number of packages in a consignment.

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN (cont.)

3.2. Mode(s) of transport

This subsection specifies the mode(s) of transport (road, rail, air, water).

4. ADMINISTRATIVE REQUIREMENTS

This section states the persons, organizations and other entities involved in the transport covered by the plan. This section also provides a detailed presentation of all of the administrative requirements that need to be satisfied to provide adequate security during the transport of the radioactive material.

4.1. Policies and procedures

This subsection lists those specific policies and procedures issued either by State entities or the responsible party that apply to the shipment(s). These policies and procedures are specified in the following:

— Policies and operational procedures for consistent implementation of security measures addressed in the transport security plan;
— Contingency plans for responding to malicious acts during transport, recovery of lost or stolen material and mitigation of consequences.

4.2. Vulnerability and threat assessment

As applicable, this subsection describes how the shipper and carrier will ensure that security measures are adequate by performing a vulnerability assessment that takes into account the threat level.

The vulnerability assessment includes a review of planned operations (equipment operability) and identification of potential vulnerabilities. This includes evaluating shipment specific parameters such as modes of transport, intermodal transfers, overnight stops and information protection.

The threat level used is described and a description of how threat level changes will be communicated and acted upon is included. Changes in circumstances that might necessitate evaluating the need for operational changes are identified in this section, such as activities that might impact routing (e.g. activists or demonstrations, road conditions, traffic conditions, secure parking for overnight trips).

4.3. Testing and evaluating the transport security plan

This subsection specifies the procedures for evaluating and testing the effectiveness of the transport security plan.

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN (cont.)

4.4. Transport security verification

This subsection describes how the shipper and carrier will ensure that all specified security measures are in place and operational prior to initiating a shipment. Any planned use of checklists for performing the pre-shipment security verification and any corrective actions are outlined here.

4.5. Notification of relevant agencies

This subsection specifies the responsibility for the timing and method of communicating notifications to relevant agencies (before, during and after transportation).

4.6. Review and update of the transport security plan

This subsection specifies when and how the reviews and updates of the transport security plan are to be accomplished.

5. PERSONNEL QUALIFICATIONS

5.1. Trustworthiness

This subsection describes the level of trustworthiness needed for personnel involved in the transport. It describes the process used to verify trustworthiness at each of those levels.

5.2. Training

This subsection specifies training qualifications for personnel involved in the transport, including the nature and frequency of the training. It also includes a description of any exercises that will be conducted as well as the schedule that will be followed for each type of exercise. A description is also included of how the results of exercises will be evaluated, including documentation of the results of the exercises and any corrective actions taken.

6. RESPONSIBILITIES

This section specifies how responsibilities are assigned and how they are transferred as shipments proceed.

6.1. Organizational structure

This subsection specifies the organizational structure of the entities involved in the transport, describing the chain of command including names of responsible personnel.

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN (cont.)

6.2. Allocation and transfer of responsibilities

This subsection describes the responsibilities of all organizations and persons engaged in the transport of radioactive material, including how and when security responsibilities are transferred.

7. INFORMATION MANAGEMENT

This section specifies the manner by which all information will be managed, particularly for security sensitive information. Reference to other information management procedures can be used.

7.1. Information security

This subsection describes how security of information will be ensured. This description might include identification of sensitive information, classification review and marking, reproduction restrictions, distribution (i.e. authorized access and need-to-know), storage requirements and destruction.

7.2. Records retention

This subsection identifies who has responsibility for retaining records to ensure records are handled in accordance with regulatory requirements and procedures (can include requirements for shippers, carriers and receivers).

8. TRANSPORT SECURITY MEASURES

This section describes the specific security measures that have been established for the shipment, addressing those measures that apply prior to transport, during transport (including storage incidental to transport) and upon receipt of the radioactive material.

8.1. Routing

This subsection specifies the routes and associated in transit storage and intermodal transfer locations. Information provided here includes the following:

— Planned (primary) and alternate routes for all modes of transport, including criteria for when the alternate routes will be used;
— Process for pre-shipment evaluation of routes, assessment of vulnerabilities;
— Identification of any in-transit storage and intermodal transfers, including security arrangements.

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN (cont.)

8.2. Transport security system

This subsection describes the security system, including specific security measures (based on the transport security level of the shipment) and other arrangements that will be used.

8.2.1. Conveyance

This subsection describes the conveyances (road, rail, air, water), including any special requirements for the conveyances.

8.2.2. Operations command and control

This subsection identifies command and control procedures for normal and emergency operations. This information includes chain of command structure, decision making authority, points of contact and identification of response agencies.

8.2.3. Nuclear security measures

This subsection identifies the nuclear security measures to be used during transport. These measures include those used to provide detection, delay and response. Examples of these measures include the following:

— Tamper-indicating devices and seals (packages and conveyances);

— Locks (single or multiple) for packages, cargo compartment and conveyance (e.g. door keys, ignition keys);

— Secure tie-downs and over-packs;

— Immobilizing devices.

This subsection also identifies the process for authorizing alternative measures (i.e. when a feature is not operational or available).

8.2.4. Communication and positional tracking for normal operations

This subsection describes the structure of the primary and alternative communication systems for the transport operation. It also describes any system for tracking the conveyances, including identification of the location at which shipment monitoring will occur.

8.2.5. Maintenance and testing of systems and equipment

This subsection addresses how all of the systems involved in the shipment(s) (such as communications and tracking) are maintained and tested. This subsection also addresses the checking and testing of all mission related equipment that will be performed prior to the beginning of the transport. It also specifies periodic testing requirements.

BOX I–2. DETAILS TO BE CONSIDERED FOR THE TRANSPORT SECURITY PLAN (cont.)

9. EMERGENCY RESPONSE

Emergency response includes both tactical and non-tactical (i.e. non-security related emergency) planning. This section identifies the range of incidents that might need response measures to be initiated, describes the appropriate response measures and clearly defines the response resources.

9.1. Emergency and contingency response

This subsection identifies handling of responses to non-nuclear or non-radiological emergency and security related incidents; it is not to be confused with specific arrangements for response to a nuclear or radiological emergency. Response actions to be included in this subsection are actions that will be taken by crew members; the transport control centre or other operations centre; shipper and receiver technical support staff; emergency response units along the route; escort personnel (if present); guard or security force (if present), and response forces.

Emergency situations can include road closure, vehicle breakdown, vehicle accidents and driver illness. Corresponding emergency arrangements could include the availability of backup vehicles and drivers, capabilities for towing and lifting, and plans for use of safe havens.

This subsection describes any necessary advance information to response forces along the route, including the time in which the communication of information has to be completed prior to the shipment. It also identifies any accompanying guard or security force.

9.2. Communications during incidents

This subsection includes a description of the communications systems and actions that will be taken to address both emergency and nuclear security events. This information could include the types of communications equipment used and features to ensure the security of communications.

9.3. Reporting of threats and incidents

This subsection describes reporting requirements, including types of events that have to be reported, to whom and how the event will be reported, and the time frame for reporting.

Annex II

TRANSPORT SECURITY VERIFICATION

II–1. Transport security verification is a mechanism that can be used to identify any deficiencies prior to conducting a shipment. The verification process can be coupled with identifying and completing corrective actions which can result in confidence that the planned transport security level is provided.

II–2. Table II–1 presents an example of security features to be verified for a shipment by road. If transport by means other than road is to be undertaken, the table will need to be appropriately modified.

II–3. Table II–1 might be useful for shipper and carrier self-assessments, as well as security audits and inspections by the regulatory body. The shipper or carrier might wish to use the table below when developing verification checklists specific to their own operations.

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT

Security features	Security arrangements verification	Pre-shipment security verification
1. DESCRIPTION OF THE MATERIAL TO BE TRANSPORTED		
Does the shipping documentation for the source or material to be transported include at least the following:		
(a) Nature, quantity, and type of material		
(b) Physical and chemical characteristics of material (weight and form of the material)		
(c) Category (according to the IAEA Code of Conduct, if applicable), or total activity per package in multiples of the applicable A_2 value if material or source is not covered in the IAEA Code of Conduct		
(d) Hazards		
(e) Packaging (description of each packaging)		
(f) Number of packages in the consignment (for each package, designation of its contents in terms of form, radionuclides and activity)?		
Has the source or material in each package been verified to determine if the radioactive content of the package meets or exceeds the activity threshold for the enhanced transport security level? (Specify details of actions taken if the content exceeds the radioactive level for enhanced security.)		
2. ADMINISTRATIVE RELATED ELEMENTS		
Has a transport security plan been developed and implemented for the transport of radioactive sources or radioactive material?		
Does the transport security plan specifically allocate responsibilities?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Does the transport security plan provide for the keeping of records of radioactive material packages or types of Class 7 radioactive material transported?		
Does the transport security plan provide for review of current operations and assessment of vulnerabilities?		
Does the transport security plan clearly state security measures and procedures that will be followed?		
Does the transport security plan clearly specify, consistent with guidance from the State, who or what organization is responsible for the plan?		
2.1. Policies and procedures		
Is a list of all relevant policies and procedures available, and are these policies and procedures known to be available to all personnel to whom they apply?		
2.2. Testing and evaluation of the transport security plan		
Has there been any testing of the transport security plan, under the direction of the transport security manager, or the designee, with company employees, contractors, carriers or other affiliated parties?		
Have drills and exercises related to the relevant plans for response to a nuclear or radiological emergency been performed? (At least annually.)		
Has the transport security manager, or the designee, determined the need for and scheduling of a security or emergency response drill or exercise related to this plan?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Were the specified security or emergency response drills or exercises undertaken, and were the results thereof properly documented in accordance with relevant quality assurance protocols?		
Has the transport vehicle been visually inspected by personnel designated by the transport security manager, or the designee, prior to departure from the shipper's facility to ensure that nothing has been tampered with and that nothing has been affixed to the packages or the transport vehicle that might affect the security of the shipment?		
Are any in-transit shipment inspections required?		
2.3. Review and update of the security plan		
Has the transport security manager, or the designee, performed a pre-shipment review of the plan immediately prior to any applicable shipment to ensure no immediate changes are needed?		
What organizations and personnel participated in the review?		
2.4. Vulnerability assessment		
Has the transport security manager, or the designee, received information that a threat level, elevated above the previous threat level evaluated, exists such that appropriate actions to revise security measures in this plan need to be implemented?		
What steps were taken to address any change in threat level? (Please describe as needed.)		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Immediately prior to each shipment, has the transport security manager, or the designee, reviewed the planned transport operations and assessed vulnerabilities considering critical factors, including the following factors (check the factors below that have been assessed):		
(a) Equipment operability		
(b) Schedule		
(c) Weather		
(d) Routes to be followed and any potential alternate routes, such that adjustments to the plan are necessary		
(e) Other (specify)?		
2.5. Threat assessment		
Has any threat, emergency, delay in transit, unusual situation, or incident for any onsite movement or offsite shipment of high consequence radioactive material been identified or reported?		
If any threat, emergency, delay in transit, unusual situation, or incident for any onsite movement or offsite shipment of high consequence radioactive material has been identified or reported, has it been reported to the appropriate personnel and authorities? (Specify details regarding what actions were taken as a result of the event that caused the reporting.)		
2.6. Reporting of threats and incidents		
Are all personnel involved in the shipment aware that any threat or incident needs to be reported immediately to appropriate management personnel?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Are methods for reporting threats and incidents specified in procedures?		
3. PERSONNEL RELATED ELEMENTS		
3.1. Allocation and transfer of responsibilities		
Are procedures and documentation available to properly control the allocation of responsibilities among involved personnel (include the establishment of commensurate authorities)?		
Are procedures and documentation available to properly control the transfer of responsibilities as follows:		
(a) Between shipper and carrier		
(b) Between carriers (if applicable)		
(c) Between carrier(s) and interim storage sites (if applicable)		
(d) Between carrier(s) and intermodal transfer facilities (if applicable)		
(e) Between carrier and receiver?		
3.2. Organizational structure		
Has the organizational structure for the shipment been appropriately documented and communicated, including specification of the chain of command and identification of responsible personnel?		
3.3. Trustworthiness		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Has the transport security manager, or the designee, ensured that personnel involved in shipments of recovered sources are trustworthy by the use of background checks prior to employment, security awareness and annual assessments of job performance?		
Is positive identification of involved personnel provided through the use of photographic identification badges?		
3.4. Training		
Does the mandatory training provided to involved personnel include the security measures per this plan?		
Is the mandatory training for all personnel involved in the shipment (vehicle drivers, guards, and response personnel) up to date?		
Are training records for all personnel involved in the shipment up to date and maintained in accordance with record keeping policies and procedures established by or through the transport security manager, or the designee?		
Have personnel been trained on the methods for reporting threats and incidents?		
4. INFORMATION MANAGEMENT		
4.1. Information security		
If the State requires advance notification of this shipment to any party, have steps been taken to ensure the security of the information contained in the notification?		
If advance notification is required, have the organizations to be notified been provided with the required advance notification information?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
4.2. Records retention		
Are all applicable records associated with this shipment (including those shown in the list below) permanently retained by the organization designated by the transport security manager, or the designee, according to existing policies established by the transport security manager, or its designee?		
(a) Training		
(b) Transport documents (including transport security plan)		
(c) Verification of sources (nuclides, activities and configuration of sources)		
(d) Source information:		
(i) When received		
(ii) How received		
(iii) Location of storage		
(e) Shippers report of:		
(i) Transfer of sources		
(ii) Authorizing signatures in accordance with procedures		
(f) Other (specify)		
4.3. Confidentiality and protection of information		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Has the transport security manager, or the designee, ensured that access to the elements of this plan have been restricted to those who have a need-to-know and that sensitive information in this plan, or otherwise associated with the recovered source shipments, has been handled in accordance with the confidentiality procedures established by or through the transport security manager, or the designee?		
5. TRANSPORT SECURITY SYSTEM		
5.1. Primary and alternate routes		
Has the transport security manager, or the designee, arranged for review and approval (by each affected public security bureau) of the schedule and both primary and alternate routes expected to be followed for the shipment of radioactive sources or radioactive material? (Specify the affected public security bureaus that have reviewed and approved the routes.)		
Are any in-transit stops anticipated? (If any in-transit stops are anticipated, document the manner by which they have been authorized and are known to be secure.)		
Has the transport security manager, or the designee, requested information on any expected delays, detours, road construction, traffic hold-ups, or weather issues that could delay transit? If information of potential delays in transit has been identified, how has it been incorporated into the transport security plan?		
5.2. Equipment related elements		
5.2.1. Equipment and modes of transport		
5.2.1.1. Packages: Are features that are important to the security of each of the packages to be transported identified, including at least the following:		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
(a) Tamper-indicating devices		
(b) Locks		
(c) Package identification numbers		
(d) External radiation levels		
(e) Others (specify any capabilities for deterrence, detection or delay)?		
Security measures on packages: Are the following security measures in place for the packages (specify the measures that are in place):		
(a) Tamper-indicating device on the packages		
(b) Locks on packages, when included in the design		
(c) Locks on package tie-downs (e.g. chains)?		
5.2.1.2. Conveyance: Is the conveyance to be used (a) a closed van type, or (b) an open, flat-bed type? [(a)] or [(b)] (Specify relevant details.)		
Is the transport vehicle owned by the carrier or is it owned by the shipper or otherwise under the control of the transport security manager, or the designee?		
Does the transport vehicle have incorporated into it any capabilities for deterrence, detection or delay?		
Security measures on conveyance: Are any of the following security measures in place on the transport vehicle? (Specify the measures that are in place.)		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
(a) Cargo compartment door of the transport vehicle, if an enclosed van type vehicle is to be used		
(b) Ignition of the transport vehicle		
(c) Door on the cab of the transport vehicle.		
Operating personnel: If transport is by road, does the transport vehicle have a driver accompanied by one or two additional appropriately qualified and equipped personnel? (Specify the number of accompanying personnel and the manner in which they are qualified and equipped.)		
If transport is by road, will each transport vehicle be accompanied by one or more escort vehicle(s), each carrying two armed or unarmed guard force personnel? (Specify the number of escort vehicles, whether the escorts are armed or unarmed.)		
Are all involved personnel instructed to ensure that the tie-downs and, as applicable, the cargo doors of the conveyance are to remain locked whenever the packages are loaded on the conveyance?		
Has the shipper provided appropriate crew members with written instructions on any required security measures, including how to respond to a security incident during transport?		
Have arrangements been made to ensure that the transport vehicle and associated escort vehicles are continuously manned during transit?		
If continuous attendance is not arranged for, have arrangements been made to secure the vehicles in a manner that complies with the principals of protection, detection and response and preferably in a well-illuminated area?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Tie-downs: If the package of radioactive sources or radioactive material are contained and carried in a closed vehicle, will the tie-downs and the cargo doors of the conveyance remain locked whenever the packages are loaded on the conveyance?		
If the package of radioactive sources or radioactive material are carried on an open, flat-bed vehicle, will the tie-downs remain locked whenever the packages are loaded on the conveyance?		
Locks: Has the integrity of all locks been verified prior to dispatch?		
5.2.1.3. Notifications:		
Has the receiver been notified of the planned shipment, mode of transport, carriers, estimated time of arrival, name of driver (or drivers), and seal/lock identification numbers?		
Have relevant State and local governments been notified, including information on routes and estimated time of arrival?		
5.2.1.4. Acceptance of shipment:		
Is the receiver prepared to:		
(a) Accept the shipment?		
(b) Verify the integrity and identification of the package(s) and conveyance?		
(c) Verify, during advance notification and in transport documents, that the carrier's and driver's identity are consistent with the information provided by the shipper and consistent with instructions from the competent authority?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
(d) Alert the transport security manager, or the designee, of any discrepancies?		
Normal operations command and control.		
Has an appropriate chain of command for the shipment been established and have all parties been made aware that, during operations associated with the transport of radioactive sources or radioactive material, the chain of command has full responsibility and authority for the shipment and any associated decisions relating to the shipment for both normal operations and emergency situations?		
Has a centralized command and control communications centre been established?		
Are centralized and continuous communications provided between:		
(a) The driver and accompanying personnel on the transport vehicle?		
(b) The driver and other escort personnel on each escort vehicle, and between all vehicles and a centralized command and control communications centre?		
Is a GPS based device or other electronic based tracking system used that communicates position of the transport vehicle to the centralized command and control communications centre and to the escort vehicle?		
Do all operating personnel have a printed booklet of all relevant telephone numbers?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Have the personnel in the transport vehicle and the personnel in its accompanying escort vehicle(s) been instructed to report to the specified centralized command and control communications centre at the departure of the shipment from the shipper site with an estimated time of arrival?		
Have the personnel in the transport vehicle or the escort vehicle been instructed that if there is any threat, emergency, delay in transit, unusual situation, or incident, it will be immediately reported, as appropriate, to the centralized command and control communications centre?		
Have procedures been established and arrangements been made that dispatch of any needed additional security and emergency resources that will be initiated and coordinated through the specified centralized command and control communications centre, and that will also initiate contact, as appropriate, with State or local enforcement officials and coordinate information management controls?		
Have the command, communication, tracking, control and emergency response plans and procedures been appropriately developed and documented?		
5.3. Additional Security Measures		
Considering the threat or nature of the material being transported, including its attractiveness, do additional security measures have to be applied? (Specify reasons for considering additional security measures.)		
If additional security measures are to be applied, specify what they are and how they have been satisfied for this shipment		
5.4. Maintenance and testing of systems and equipment		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Has an operability and functionality procedure for all equipment and communication devices to be used in the shipment been established?		
Has the operability and functionality of all equipment and communication devices to be used in the shipment been performed in accordance with the established operability and functionality procedure?		
What equipment and communication devices have been tested that apply to this security plan?		
Have procedures for testing and maintaining the transport vehicle been established?		
Has the maintenance and testing of the transport vehicle been performed in accordance with the established procedure?		
What equipment that applies to this security plan has been maintained and tested, and did the maintenance and testing satisfy all of the specifications established in the relevant maintenance and testing procedure?		
6. EMERGENCY RESPONSE		
Has an emergency response manual been developed that applies to this shipment (it might be a separate emergency response manual or part of a more comprehensive security manual)?		
6.1 Non-tactical and tactical emergency response		
Are local law enforcement organizations aware that they are to provide armed response in the event of an incident, including a security attack?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Are the transport vehicle crew and the escort vehicle personnel aware that the procedures in the emergency response manual have to be followed in case of an incident, including a security attack?		
In the case of any emergency or security threat, breach of security or other security incident, are the emergency response organizations aware that, if required, any needed medical action has to be taken in accordance with applicable procedures in the emergency response manual?		
In the case of any emergency or security threat, breach of security or other security incident, do both the crew of the transport vehicle and the escort vehicle car have in their possession the emergency response procedures defining the actions to be taken?		
Has an arrangement been made and procedures been established with an applicable radiation protection agency to provide appropriate and timely response in the case of a security attack or an incident?		
6.2 Incident communications		
In the case of any emergency or security threat, breach of security or other security incident, has contact information for non-security related events been provided to involved personnel using the emergency response manual?		
Are the transport vehicle crew and the escort vehicle personnel aware that, in the case of an incident, including a security attack, they have to immediately contact the specified centralized command and control communications centre, providing detailed information regarding the attack?		
Has a centralized point of contact been arranged for establishing, with the State or local enforcement officials, appropriate and timely response in the event of a security attack or an incident?		

TABLE II–1. EXAMPLE SECURITY FEATURES TO BE VERIFIED FOR ROAD TRANSPORT (cont.)

Security features	Security arrangements verification	Pre-shipment security verification
Upon notification by the transport vehicle crew and escort vehicle personnel of a security attack or an incident, is the specified centralized command and control communications centre aware that they have to immediately contact the relevant response force centralized point of contact defined in the transport security plan, and provide detailed information regarding the attack?		
Upon notification by the transport vehicle crew and escort vehicle personnel of a security attack or an incident, is the relevant response force centralized point of contact defined in the transport security plan aware that they have to contact, as needed, response forces (including military, if needed) to ensure adequate and timely mobilization of these forces?		
In the case of a security attack or an incident, is the relevant centralized point of contact aware that they have overall responsibility for handling the tactical response at the scene of the attack in their bureau?		
In the case of a security attack or an incident, is the relevant involved radiation protection agency aware that they have to be responsible for addressing radiation protection issues at the scene of the security attack or incident?		
6.3 Notification of relevant agencies		
Has the receiver agreed to notify the shipper if the consignment is not received as anticipated?		

Annex III

CROSS-REFERENCE OF MODE INDEPENDENT SECURITY MEASURES

III–1. Table III–1 provides cross-references to the specific security measures listed in paras 5.10–5.69. It provides a listing of mode independent security measures in the left column and across each row provides the paragraph numbers where information about the security measure can be found in this publication.

TABLE III–1. CROSS-REFERENCE OF SECURITY MEASURES TO PARAGRAPH NUMBERS

Mode independent security measure	Basic transport security level (5.8, 5.9)	Enhanced transport security level (5.31)	Additional security measures (5.53)
Evaluation and exchange of security related information	5.10		
Protection and control of security related information	5.11	5.32, 5.33	
Trustworthiness determination	5.12, 5.13		5.54
Written instructions, procedures and plans	5.14	5.34–5.38	5.55, 5.56
Security training	5.15–5.17		5.57
Shipper and carrier credentials/identification/ licensing	5.18	5.39	5.58
Receiver/carrier authorization	5.19	5.40	
Planning and coordination		5.41–5.43	
Advance notification			5.59
Communications	5.20	5.44, 5.45	5.60–5.62
Open, closed and special conveyance considerations	5.21	5.46–5.48	5.63–5.65
Conveyance inspections	5.22		5.66
Package and conveyance security systems	5.23		
Monitoring and tracking the shipment	5.24	5.49	5.67

TABLE III–1. CROSS-REFERENCE OF SECURITY MEASURES TO PARAGRAPH NUMBERS (cont.)

Mode independent security measure	Basic transport security level (5.8, 5.9)	Enhanced transport security level (5.31)	Additional security measures (5.53)
Guards and individuals accompanying the shipment			5.68, 5.69
Pre-shipment security verification		5.50–5.52	
Continuity of security measures	5.25–5.27		
Receipt verification	5.28–5.30		

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

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

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

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

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978-92-0-112110-3 Price: €22.00

CATEGORIZATION OF RADIOACTIVE SOURCES
IAEA Safety Standards Series No. RS-G-1.9
STI/PUB/1227 (55 pp.; 2005)
ISBN 92-0-103905-0 Price: €18.00

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10
STI/PUB/1386 (30 pp.; 2009)
ISBN 978-92-0-102509-8 Price: €18.00

SECURITY OF RADIOACTIVE MATERIAL IN USE AND STORAGE AND OF ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 11-G (Rev. 1)
STI/PUB/1840 (105 pp.; 2019)
ISBN 978-92-0-110018-4 Price € 50.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8-G (Rev. 1)
STI/PUB/1858 (37 pp.; 2020)
ISBN 978-92-0-103419-9 Price € 24.00

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7
STI/PUB/1347 (37 pp.; 2008)
ISBN 978-92-0-107808-7 Price: €30.00

SECURITY OF NUCLEAR MATERIAL IN TRANSPORT
IAEA Nuclear Security Series No. 26-G
STI/PUB/1686 (104 pp.; 2015)
ISBN 978-92-0-102015-4 Price € 48.00

This publication is an update of IAEA Nuclear Security Series No. 9 and serves as Implementing Guide for the IAEA's Nuclear Security Recommendations on Radioactive Material and Associated Facilities. It provides guidance to States and their competent authorities on how to establish or improve, implement, maintain and sustain the elements of the nuclear security regime to protect transport of radioactive material against unauthorized removal and sabotage. It may also be useful to shippers or carriers of radioactive material in the design and implementation of their security systems. The publication provides guidance on the implementation of security measures in a graded manner, taking into account the level of threat, the relative attractiveness of the material, the safety–security interface and the potential consequences resulting from malicious use.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA