IAEA NUCLEAR SECURITY SERIES NO. XX

NST053

STEP 8: Soliciting comments by Member States

SECURITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL IN TRANSPORT

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

FOREWORD

(foreword to be inserted)

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 The IAEA Nuclear Security Series provides guidance for States to assist them in implementing national nuclear security regimes as well as in reviewing and, when necessary, strengthening their regimes. The series also provides guidance for States in fulfilling their obligations and commitments with respect to binding and non-binding international instruments adopted under the IAEA and other auspices.

1.2 IAEA Nuclear Security Series No. 20 Objective and Essential Elements of a State's Nuclear Security Regime [1] provides the objective and essential elements for a nuclear security regime. The IAEA Nuclear Security Recommendations indicate what a nuclear security regime should address in IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3] and, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [4].

1.3 The Recommendations on the transport of dangerous goods-Model Regulations [5] provide recommendations 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. The security provisions for the transport of dangerous goods are found in Chapters 1.4 and 7.2 of the UN Model Regulations [5].

1.4 Other UN specialized agencies and programmes have taken similar steps to support improved security in the transport of dangerous goods during specific modes of transport. The International Maritime Organization, the International Civil Aviation Organization and the United Nations Economic Commission for Europe, the Intergovernmental Organization for International Carriage by Rail and the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways have all amended their respective international instruments [6–8] 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 [9], [10] 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 Reference [2] provides recommendations on the physical protection of nuclear material in use, storage and transport. IAEA Nuclear Security Series No. 26-G, Security of Nuclear Material in

Transport [11] provides detailed guidance on how to implement the recommendations for the security of nuclear material in transport provided in Ref. [2]. Paragraph 1.3 of Ref. [11] states that:

> "This Implementing Guide is therefore intended to assist States' competent authorities and shippers or carriers to fulfil their physical protection responsibilities in the transport of nuclear material. Where the term 'shipper or carrier' is used in Ref. [11], it refers to the entity to which any specific physical protection responsibility related to transport is assigned."

1.7 Reference [3] provides recommendations for the security of radioactive material throughout its lifecycle, including during transport. IAEA Nuclear Security Series No. 9-G (Rev. 1), Security of Radioactive Material in Transport [12] provides guidance for establishing transport security levels for radioactive material in transport and for establishing security measures against unauthorized removal and sabotage of radioactive material in transport.

1.8 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] and GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [15].

1.9 Technical advice and practical information for the management of the interface between nuclear safety and nuclear security during normal commercial shipments of radioactive material is provided in IAEA Technical Reports Series No. 1001, Managing the Interface between Safety and Security for Normal Commercial Shipments of Radioactive Material [13].

OBJECTIVE

1.10 The objective of this publication is to provide detailed guidance to States and their competent authorities[1] on how to implement and maintain a nuclear security regime for the transport of nuclear and other radioactive material. This publication may also be useful to operators, shippers, carriers, and others with transport security responsibilities in designing their transport security systems.

1.11 This publication builds on the relevant recommendations in Refs [2], [3] and provides additional, explanatory on how to implement these recommendations in practice. This publication complements the guidance provided in Refs [11], [12].

[1] A governmental organization or institution that has been designated by a state to carry out one or more nuclear security functions.

SCOPE

1.12 This publication applies to the security of nuclear and other radioactive material during transport and provides guidance for protection against unauthorized removal and sabotage during transport.

1.13 This publication also describes the specific nuclear security measures to locate and assist in the recovery of lost, missing, or stolen nuclear and other radioactive material. More detailed guidance on this topic can be found in Ref. [4]. This publication does not address the emergency arrangements pertaining to the response to a nuclear or radiological emergency involving such material. This topic is covered in Refs [16]–[20].

1.14 Security measures and safety measures for the transport of nuclear and other radioactive material should be implemented in a coordinated manner in accordance with Ref. [13] 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 No. SF-1, Fundamental Safety Principles [23] states 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".

1.15 While detailed guidance on transport specific measures with respect to the protection of security related information and computer security measures is provided in this publication, additional information may be found in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [24] and 42-G, Computer Security for Nuclear Security [25].

1.16 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.

STRUCTURE

1.17 Section 2 provides an overview of nuclear and radioactive material categorization. Section 3 provides guidance on the responsibilities of the State in establishing a transport security regulatory regime. Section 4 provides guidance on the design, evaluation and implementation of a nuclear security system for material in transport. Section 5 provides guidance on the implementation of security measures. Section 6 provides guidance on the development, implementation and evaluation of a transport security plan. Finally, Section 7 provides guidance on managing international and regional transport.

2. OVERVIEW OF NUCLEAR AND RADIOACTIVE MATERIAL CATEGORIZATION SYSTEMS AND ASSIGNMENT OF TRANSPORT SECURITY LEVELS

2.1. A categorization system should be applied to implement a graded approach to the safety and security of nuclear and other radioactive material in transport. This section considers the most widely used categorization schemes for nuclear and other radioactive material in transport, the primary purpose for which they were intended to be used, the technical basis for their use, and how they are applied. An overview of the categorization systems is provided in TABLE 1. Further explanations for each system can be found in Refs [2, 5, 12, 13, 14, 26].

2.2. References [2], [11] are aligned with the nuclear material categorization presented in the Convention on Physical Protection of Nuclear Material [9] and provide recommendations on specific transport security measures for each category of nuclear material. More specifically, para. 4.5 of Ref. [2] states that:

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

2.3. The recommendations in Refs [2, 3, 11, 12] on transport security for radioactive material are consistent with the UN Model Regulations [5] ('Class 7 - Radioactive material'). The UN Model Regulations [5] use a threshold to differentiate between high consequence radioactive material packages and other radioactive material packages, and provide requirements on the security of dangerous goods in transport in all modes as follows:

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

2.4. Reference [12] states:

> "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. [26]], an activity equal to or exceeding that for a Category 2 radioactive source[6] (ten times the D value);
> (b) For all other radionuclides, an activity of $3000A_2$ or greater".

"3.12. A State should also define which radioactive material poses very low potential radiological consequences if subject to unauthorized removal or sabotage and thus does not represent a substantial security concern. Packages containing such material do not need to be assigned a transport security level and only need to be controlled through prudent management practices."

"[6] Radioactive sources with activities between 10D and 1000D are also referred to as Category 2 and greater than 1000D are referred to as Category 1. Further detailed guidance can be found in Ref. [16]."

2.5. Appendix I of Ref. [12] describes three transport security levels: prudent management practices, basic transport security level, and enhanced transport security level. It also describes the method by which A_2 and D values are used to define the activity threshold for assigning radioactive material to a transport security level.

2.6. For prudent management practices, "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." [12]. The basic transport security level and the enhanced transport security level, more stringent security measures are recommended.

2.7. During transport, different materials may be present in the same conveyance[2] or combined on multiple conveyances as part of a convoy. Thus, there is frequently a need to assign a transport security level to an aggregation of nuclear or other radioactive material (see paras 4.6–4.17 of Ref. [11] and paras 3.26–3.28 of Ref. [12]). Detailed guidance on how to calculate the category of an aggregation for nuclear material can be found in paras 4.6–4.17 of Ref. [11] and for other radioactive material in paras 3.26–3.28 of Ref. [12].

[2] Conveyance is defined [14] as follows: (a) For *transport* by road or rail: any *vehicle*; (b) For *transport* by water: any *vessel*, or any hold, compartment, or *defined deck area* of a *vessel*; (c) For *transport* by air: any *aircraft*.

TABLE 1. WIDELY USED CATEGORIZATION SYSTEMS AND TRANSPORT SECURITY LEVEL ASSIGNMENTS FOR THE SAFETY AND SECURITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL IN TRANSPORT.

Material Categorization and Transport Security Level Assignment	**Purpose**	**Technical Basis**	**Application in Transport**
Nuclear material: Nuclear material categories I, II and III Source: Refs [9], [10], [2], [2]	To assign physical protection levels to protect nuclear material against unauthorized removal (para. 4.2 of Ref. [2], para. 4.4 of Ref. [2] para. 4.4)	Potential for the material to be used in a nuclear explosive device based on the element (uranium, plutonium), radionuclide, quantity, enrichment level for U-235, and irradiation (if applicable)	Direct application
Radioactive material: Basic transport security level and enhanced transport security level; prudent management practice and additional security measures Source: Ref. [12]	To define transport security levels and to specify security measures to be applied for radioactive material within each transport security level	Transport security measures applied should follow a graded approach which varies in depth and rigor commensurate with the threat and the potential radiological consequences resulting from a malicious act involving radioactive material (see appendix I of Ref. [12])	Direct application
Radioactive sources: Radioactive source categories 1, 2, 3, 4 and 5 and D values Source: Refs [12], [27], [26]	To provide a simple, logical system for ranking radioactive sources in terms of their potential to cause harm to human health (see para. 1.8 of Ref. [27])	Although sources with an activity exceeding the D values are considered dangerous, it is not considered realistic to implement enhanced security measures for all sources with an activity exceeding the D values. 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 (see appendix I of Ref. [12], [26])	Indirect application (see Dangerous goods transports below)

Material Categorization and Transport Security Level Assignment	Purpose	Technical Basis	Application in Transport
Transport safety: A_1 and A_2 values Sources: Refs [14], [28]	"The Q system define the 'quantity' limits, in terms of A_1 and A_2 values, of a radionuclide that is allowed in a Type A package". (para I.1. of appendix I of Ref. [28])	The Q system considers a series of exposure routes (internal or external), of persons in the vicinity of a Type A package, involved in a severe transport accident (paras. I.8 and I.14 of Ref. [28])	Direct application for transport safety regulations Indirect application for security (see Dangerous goods transports below)
Dangerous goods transports: All dangerous goods and high consequence dangerous goods and corresponding security provisions Source: Ref. [5]	To specify the security provisions that have to be applied for the conveyance, shipment and/or package of radioactive material	The activity threshold for the application of the enhanced security level is 10D for the radionuclides listed in the Code of Conduct [26] and $3000A_2$ for all other radioactive materials	Direct application

3. DEVELOPING AND IMPLEMENTING A TRANSPORT SECURITY REGIME

3.1. This section provides guidance for States developing and implementing a transport security regime in accordance with their legislative framework for the security of nuclear and other radioactive material in transport. Detailed guidance on how to develop regulations and additional administrative measures for nuclear security is provided in IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security [29].

DEVELOPING REGULATIONS FOR TRANSPORT SECURITY

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

3.3. A transparent process for the development of transport regulations and clarity on the roles and responsibilities of all stakeholders helps to facilitate the understanding and use of the regulations by operators, shippers and/or carriers. During this process, a good practice would be to establish a drafting committee who will work with relevant authorities to ensure all transport security laws, requirements,

agreements, and conventions observed by the State are accounted for in the regulations for transport security. This drafting committee may include legal and technical specialists from the relevant competent authorities.

3.4. These regulations should be developed to account for all modes of transport (i.e. road, rail, air and water) and for domestic and international transport. The chain of custody and responsibility to ensure accountability for the package during transport should be considered in the development of regulations. It should be ensured that the required level of security is maintained throughout the entire duration of the shipment, including during intermodal transfers, interim storing, and/or where there might be a transfer of custody or changeover of the security responsibility between different operators, shippers and/or carriers.

3.5. Any operating conditions or equipment specific to the mode of transport used within the State should be identified and should be taken into account in the development of the regulations to ensure that the regulations can be applied in a cost-effective, practical and realistic manner.

3.6. In the transport security regulations, it should be ensured that all responsible competent authorities and operators, shippers and/or carriers have clearly defined roles and responsibilities based on the functions they perform and consistent with the type of material and mode of transport used.

Developing a comprehensive understanding of transport within the State

3.7. Before starting to develop transport security regulations, the competent authority should have a comprehensive understanding of the nature and the uses of nuclear and other radioactive material within the State as well as the threat to such material, to identify the types of shipment that will be subject to the regulations. This understanding helps the competent authority to identify the major shippers, carriers and receivers in the State, as well as the type of material, the frequency and the modality of transport.

Examining other national regulations, agreements and other associated administrative measures

3.8. The competent authority should have a clear understanding of the applicable international requirements and should examine other national regulations, agreements and other associated administrative measures to identify existing security measures or processes that could be used to meet transport security objectives to prevent duplication of effort and promote harmonization among different regulations. For example, if trustworthiness verification is already conducted by another competent authority, the existing process or information gathered could be used to verify or accept the trustworthiness of persons that will be engaged in transport security. Other existing regulations (e.g. on transport safety, environmental protection, emergency response) should also be taken into account when allocating roles and responsibilities for transport security, to ensure a compatible allocation of responsibilities for operators, shippers and carriers.

3.9. The State may already have regulations that cover the identification and protection of sensitive information and set out levels of information sensitivity and accepted methods for developing, reproducing, granting access to, transmitting, storing and destroying sensitive information. The competent authority may be able to use these regulations when developing requirements for transport security plans, security measures, routes, contingency plans, emergency response plans and the transmission, storage and handling of sensitive information.

Consulting with stakeholders

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

3.11. After the regulations are drafted, the competent authority should, if legally permissible, provide sufficient opportunities to all relevant stakeholders to comment on the draft regulations and to present any perceived challenges they might face in the practical implementation of the regulations. After these challenges are identified, the competent authority could redraft the relevant requirements, as practical, to mitigate these challenges.

3.12. During this consultation process, if legally permissible, the competent authority should respond to public comments in an open and transparent manner. This approach provides the opportunity to the competent authority to clarify prescriptive requirements and/or performance objectives and avoid potential misinterpretation of the regulations. This approach establishes a clear line of communication between the competent authority and the stakeholders that can enable the efficient implementation of the regulations.

3.13. After promulgation of the regulations by the State, the competent authority should communicate the regulations, their content and the relevant enforcement mechanisms to the public and operators taking into considerations the requirements for protection of information. This communication may be accomplished by conducting outreach activities with relevant transport stakeholder groups to facilitate communication amongst them.

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

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

(a) Ensure compatibility between transport regulations in shipping, receiving and transit States;

(b) Streamline the preparation of international shipments and the transport approval process through bilateral and multilateral agreements;

(c) Minimize potential security lapses due to conflicting or incomplete requirements when international shipments enter or exit the State;

(d) Minimize radiation exposure of workers and the public due to potential shipment delays and additional in-transit storage time;

(e) Reduce the risk of loss, diversion, or theft of nuclear and other radioactive material during transport due to potential shipment delays and additional in-transit storage time;

(f) Avoid denial or delay of shipments due to problems with ensuring compliance with different requirements; and

(g) Reduce the operational costs by minimizing denial or delay or shipments.

REGULATORY OVERSIGHT FOR TRANSPORT SECURITY

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

3.16. The competent authority should develop a regulatory oversight programme with the following basic functions: licensing and authorization, inspections and enforcement.

3.17. The legislative and regulatory framework should clearly describe the activities to be undertaken by the competent authority as part of its regulatory oversight responsibilities and should grant the necessary legal authority to the personnel of the competent authority to conduct inspections for transport security in order to verify compliance with "applicable licence conditions, including compliance with the [transport security plan]" [11].

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

3.19. The competent authority should review findings resulting from inspections, to assess the performance of all elements of the transport security system, and investigate non-compliances and to determine if any corrective actions are needed.

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

3.21. Depending on the purpose and objectives of the inspection, the inspections may investigate the following elements of the transport security system of the licensee:

(a) Security systems put in place at transhipment point, temporary storage or on conveyances or loads;
(b) Administrative elements, such as information security, personnel security or staff training and competency;
(c) Transport security plans, contingency plans, response plans, tracking arrangements, communication arrangements, arrangements and capabilities for escort, guard and response forces;
(d) Security exercises and tests, including route selection and planning.

3.22. There are three main types of transport security inspections of designated sites, activities and conveyances: (a) announced or routine inspections; (b) unannounced inspections that have been coordinated with the licensee in advance; (c) reactive, short-notice inspections as a result of information received or of a security event. These inspections may be conducted in several locations, including operator headquarters, storage facilities, conveyance loading areas, temporary or in-transit stops, transhipment points and final destinations. The location of the inspection depends on the purpose and outlined objectives of the inspection. Unannounced transport security inspections should be carefully planned by the competent authority and coordinated with escort, guard and response forces if any.Inspectors should have appropriate training, thorough knowledge of the relevant regulatory requirements and of the licence conditions, practical knowledge of the security elements to be inspected and knowledge of interfaces with other areas, such as radiation protection, emergency planning and transport safety requirements. For example, for inspections on the arrangements for escort, guard and response forces, the inspector should have an in-depth understanding of the relevant national requirements and some knowledge on convoy and response forces; while for inspections on the administrative arrangements for an international shipment, the inspector should be familiar with the transport security requirements in the transit States, as well as with any legally binding regional or international requirements.

3.23. Planning should be conducted using a graded approach and the purpose of each inspection should be clearly stated. Preparing for an inspection includes a detailed review of the approved transport security plan, if applicable, relevant information from other competent authorities, an estimation of the duration of the inspection, notification of the persons to be involved in the inspection, administrative

arrangements and preparation of the equipment to be used in the inspection. An inspection checklist[3] can help with ensuring that the inspection is complete and thorough.

3.24. An inspection may begin with an initial meeting between the competent authority and the shipper and/or carrier managers or representatives to explain the purpose and the scope of the inspection. The inspection activities should be conducted against the approved transport security plan and the relevant transport security regulations. Findings, facts, assessments and recommendations should be clear, logical and supported by evidence and should be recorded by the inspector and included in the inspection report. The report should also identify good practices and non-compliances and their safety and security significance. Inspection reports should be peer reviewed and shared with relevant stakeholders, as appropriate, taking into account the need for information security, to enable them to be informed and support decision making. Inspection reports should be stored, archived and appropriately protected.

3.25. Following an inspection, the inspector should clearly indicate whether any follow up action is needed. If action is needed, this may be in the form of a major or minor non-compliance issue needing enforcement and possible immediate correction. Depending on the severity, a shipper's and/or carrier's licence or authorization to operate may be suspended or terminated. Following an inspection, relevant good practices as well as, where appropriate, examples of findings and corrective actions taken to mitigate non-compliance, should be shared with shippers and carriers as well as others with a need-to-know who may benefit from the knowledge.

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

3.27. Recording and distributing findings, assessments and recommendations relating to transport security can be used to give directions to shippers and/or carriers, and to support the enforcement of actions to be considered or taken.

4. DESIGNING AND EVALUATING A TRANSPORT SECURITY SYSTEM

4.1. This section provides guidance on designing, evaluating, implementing and maintaining a transport security system.

[3] The IAEA has developed an example inspection checklist available to Member States upon request.

4.2. States use three different approaches for specifying security requirements: the prescriptive approach, the performance based approach and the combined approach. Paragraph 4.3 of Ref. [12] states:

> "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."

4.3. In the prescriptive approach, the transport security measures applied are required to comply with the administrative and technical requirements specified in the national regulations. In the performance based approach, the transport security system is required to be designed to meet the national security objectives (example, national threat assessment or design basis threat) taking into account the national nuclear security threat assessment, design basis threat and representative threat statements. Many States select a combined approach which allows for different design approaches to be used by licensees.

4.4. When the performance based approach or the combined approach is used for the design of transport security systems, a systematic approach is followed [30],[31]. The systematic approach comprises the following three phases:

(1) Phase 1, where the operator identifies the requirements for the transport security system in accordance with the national security objectives, requirements and specifications. It includes steps such as target identification, assessment of the threat information.

(2) Phase 2, where the operator designs the transport security system. It includes steps such as considering the conveyance configuration and the design of the security system, including measures for detection, delay and response.

(3) Phase 3, where the operator analyses and evaluates the effectiveness of the transport security system. It includes steps such as conducting vulnerability assessments, performance testing and scenario analysis.

4.5. The results of Phase 3 determine if the design is ready for implementation, whether the existing system is adequate or if a new design is needed. If the national security objectives or design specifications defined in Phase 1 are not met by the outputs of Phase 3, the new system should either have to be re-designed or the existing system should have to be enhanced with emphasis on the weak areas identified by the Phase 3 analysis.

4.6. The sequencing of these three phases and a summary of the activities included under each phase are illustrated in FIG. 1, which has been adapted from fig. 1 of Ref. [31] to transport security systems, and a more detailed explanation of the three phases is provided in paras 4.7–4.29.

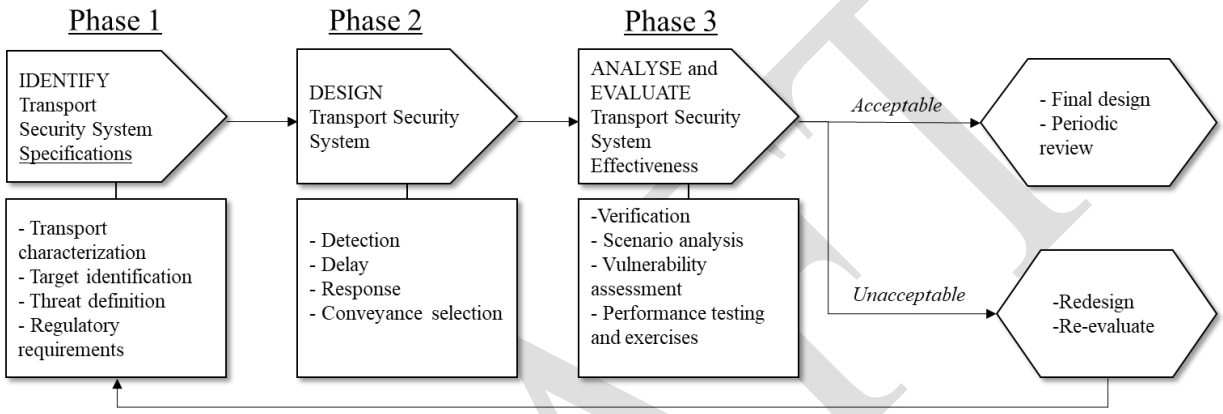

FIG. 1. Process for the design and evaluation of a transport security system.

PHASE 1: IDENTIFYING SPECIFICATIONS FOR THE TRANSPORT SECURITY SYSTEM

4.7. During Phase 1, the operator should develop appropriate documentation to identify the security specifications for the conveyance and other elements of the transport security system (e.g. escort vehicles, communication devices, security personnel equipment, layout and equipment of the transport control centre) and to set out the specifications for normal operations and contingency situations. The following considerations might be considered in this documentation:

(a) Security specification;
(b) Target identification;
(c) Threat information;
(d) Regulatory requirements and other international or national standards.

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

4.9. The operator should conduct an analysis to evaluate the characteristics of the material to be transported and the environment surrounding the shipment, such as the potential threats and the robustness of the transport infrastructure. To identify potential threats, the analysis should integrate

information provided by law enforcement, intelligence agencies, relevant security agencies and other relevant competent authorities.

PHASE 2: DESIGNING THE TRANSPORT SECURITY SYSTEM

4.10. During Phase 2, the operator should design the transport security system, taking into account the results of the analysis conducted in Phase 1. The design of the transport security system should include measures to provide the functions of detection, delay and response (see in Ref. [12]).

Selecting the conveyance

4.11. Selecting the conveyance can be complex due to the safety hazards and security threats associated with the transport of nuclear and other radioactive material, the operational life cycle and the maintenance needs of the conveyance, the operational conditions of the security system, as the type of road, the weather conditions and the needs of the users of the conveyance. The safety and security systems of a conveyance are closely linked on a single platform that needs to operate while in motion, making it necessary to consider the interactions between transport safety and transport security elements.

4.12. The operator should consider general specifications for the conveyance including load handling capacity, number of personnel needed to operate the conveyance, its gross weight, physical dimensions and operational speed.

4.13. The operator should consider specifications for normal operations and emergency situations. Normal operations refer to the routine use of the conveyance, without any particular safety or security concerns. The emergency situations involve operation under specific safety and security concerns which the conveyance might encounter during use, including planned response to nuclear security events. Emergency situations may include collisions of the conveyance with other vehicles, vessels or aircraft, fires (either as the result of a collision or from some other abnormal event) and/or breakdown of the conveyance.

4.14. Maintenance specifications should outline how frequently routine maintenance has to be performed and which components have to be replaced. Preventive maintenance should also be performed. Lifecycle specifications concerning the expected useful life of the conveyance, from production through decommissioning and disposal, should also be considered.

4.15. Specifications for security during storage while not in use, temporary storage, and in transit storage should also be considered, taking into consideration any specific considerations relating to the conveyance. The requisite level of security of the conveyance and/or package should be maintained until it is needed for the next movement of material.

PHASE 3: ANALYSING AND EVALUATING THE EFFECTIVENESS OF THE TRANSPORT SECURITY SYSTEM

4.16. During Phase 3, the operator should analyse and evaluate the performance of the designed transport security system to assess whether it meets the security objectives with respect to the threat assessment for the conveyance. The methods for evaluating the performance of the transport security system are outlined in paras. 4.820–4.29. The selection of the method depends on the national regulatory requirements, the technical capabilities of the operator and the resources allocated to complete the analysis.

4.17. If the prescriptive approach or other variant of the combined approach has been used to define the security requirements, the operator should verify that the transport security system meets the prescriptive requirements.

4.18. For the performance based approach, after the analysis of the effectiveness of the transport security system is complete, transport security experts with specific, applicable knowledge of the individual equipment and components that make up the transport security system should conclude whether or not the transport security system meets the defined performance objectives. As an example, the analysis might conclude that the transport security system is unable to meet its performance objective to delay an adversary long enough for the response forces to arrive. If the designed system does not meet the defined performance objectives and is not considered acceptable, an upgrade or re-evaluation should be undertaken. An upgrade implies an improvement to existing security measures or implementation of additional security measures in order to meet the performance objectives without redesigning the whole transport security system.

4.19. The transport security system should be regularly analysed and evaluated, even in cases where the initial analysis determines that the transport security system meets the performance objectives. This is to ensure that the system continues to be effective when threats change, technology becomes aged or obsolete, or additional regulatory requirements are imposed.

Use of scenarios in evaluating the effectiveness of the transport security system

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

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

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

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

(a) Identifying the potential vulnerabilities of the convoy, such as vulnerabilities associated with the conveyance, the route and the transport security system;
(b) Creating a detailed list of tasks that the adversary has to complete to achieve its goal, beginning with the initiation of the attack;
(c) Creating a plan to describe how the adversary can accomplish the tasks identified in the previous step, including times needed for completion of each task;
(d) Examining the multiple attack plans.

4.23. Once the scenarios are fully developed and/or made available through the competent authority (including the adversary attack plan), they can be used to conduct either a vulnerability assessment or an exercise, as described in the paras. 4.24–4.29.

Vulnerability assessment

4.24. A vulnerability assessment is a systematic methodology for analysing the performance of administrative and technical measures that can be used to evaluate the specifications of a transport security system against the national threat assessment or design basis threat. In particular, a vulnerability assessment is typically used by the operator to determine the effectiveness of security technologies and protection strategies employed in the proposed security system, define its strengths and weaknesses and develop cost-effective and balanced upgrades. Additional information on the vulnerability assessment methodology for the security of nuclear material in transport, also applicable to other radioactive material, can be found in paras. II.1–II.21 of Ref [11].

Performance testing and exercises

4.25. Limited scope performance testing and exercises are two methods used by the operator for testing the performance of the transport security system.

4.26. Limited scope performance testing involves the examination of a specific element of the transport security plan ensure that the security measures associated with this element function as designed. For example, one might test the communication system or a set of procedures.

4.27. Exercises are scenario-based performance tests, such as drills, table-top exercises and field exercises that use a realistic and credible scenario consistent with the threat assessment and/or design basis threat to evaluate the performance of any aspect of the transport security plan**.** More detailed information regarding transport security exercises can be found in Ref. [32].

After-action review

4.28. After the shipment has been successfully conducted, the licensee should review if there were any gaps or vulnerabilities during the shipment and, if applicable, consider potential improvements that could be implemented in future transport operations. This concept is typically associated with quality assurance or quality improvement process. Competent authorities, licensees and possibly law enforcement should participate in a review process to identify areas for improvements in areas such as regulatory oversight, transport security planning processes, effectiveness of operational security and specific nuclear security response measures.

4.29. Debriefs or surveys are methods that could be employed for this review by requesting from organizations to collate and share the lessons identified to embed good practices and make improvements in future shipments. Debriefs may be conducted by all relevant organizations immediately after a shipment.

5. IMPLEMENTING TRANSPORT SECURITY MEASURES

5.1. In accordance with paras 5.24–5.30 of Ref. [11] and paras 4.14–4.29 of Ref. [12], the functions of a transport security system are the following:

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

(b) Detection which includes activities to provide for early detection and assessment of a malicious act against a shipment of nuclear and other radioactive material;
(c) Delay which includes activities to prevent access or impede attempts of malicious acts;
(d) Provide notification to the appropriate authorities of:

1) attempts of, or actual malicious acts,
2) responses to interrupt the malicious acts and
3) efforts to assist in the recovery of the material of a successful malicious act.

The integrated set of transport security measures implemented to fulfil these security functions makes up the transport security system.

5.2. When implementing a transport security system, the interactions between the three security functions should be considered. For example, without timely detection, delay measures might be less effective, because the adversary will have more time to overcome the protection measures; without sufficient delay, there might not be enough time to provide for an effective response. For most shipments, in case of a security event, response forces might need to arrive at the location of the shipment from some distance away from the shipment.

5.3. In a transport security system, security measures can fulfil more than one security function. For example, a lock typically provides a delay function during an attack but can also be used to detect attempted theft after the shipment has been concluded; escort forces can detect a malicious act and also provide response functions.

5.4. Additional security measures may be warranted for certain shipments, depending on the category, type or quantity of nuclear or other radioactive material, on the nature of the threat, on the capabilities and intent of the potential adversaries, or if a shipment is particularly difficult or sensitive due to criteria determined by the State. For example, situations that warrant additional security measures might include shipments during a major public event (e.g., sporting or political event), shipments during on-going political or social unrest, shipments through extremely remote or extremely populated areas, or shipments through areas of poor governmental control.

5.5. Shippers or carriers can make use of national and international standards for detection equipment, protection equipment, protective equipment and communication devices as references when designing and implementing their transport security systems.

5.6. Transport security measures may comprise technical measures (e.g. locks, seals, armour, intrusion detection equipment) and administrative measures (e.g. responsibilities, procedures, number of personnel) that can be implemented during transport. Paragraphs 5.7–5.71 describe such measures for the conveyance, the escort and the transport control centre. Paragraphs 5.72–5.89 provide guidance for

the communications systems and for the training and qualification of the personnel for transport security systems.

TRANSPORT SECURITY MEASURES RELATING TO THE CONVEYANCE

Technical measures

Tamper indicating devices

5.7. A tamper indicating device is a device that, when applied to conveyances, cargo compartments, packages, freight containers or critical security controls, provides a means of detecting unauthorized access or tampering. Seals are one type of tamper indicating device applied to packages, overpacks and freight containers that make up an integral part of the approved shipping configuration to detect potential unauthorized access to the material. Operators may have to use specific seals or may be restricted from modifying the transport package to add more seals or change seal types. The selection and application of seals should be integrated into the transport security planning process and meet the applicable regulatory requirements.

5.8. The following practices should be followed when seals are used as tamper indicating devices:

(a) Documentation should be retained and filed from the manufacturer proving what type of seal was purchased and the security features it has;
(b) An inventory should be maintained of all seals purchased and stored;
(c) Documentation should be recorded for each seal that is affixed, destroyed, or removed;
(d) Seals should only be issued to and affixed by authorized company employees or agents;
(e) Procedures should be established for reporting tampered seals that are discovered throughout the supply chain;
(f) Procedures should be put in place for retaining or disposing of used seals that have been removed;
(g) Specific training should be provided for employees, contractors, or agents that issue, affix and dispose of seals.

5.9. In addition, a published international or national standard[4] should be followed in the selection of the seals to assist the designers of transport security system in selecting appropriate seals and in ensuring the seals selected display the needed level of performance. The standard used should provide information on three major features of seals considered for selection: a test of physical strength of the

[4] The term 'standard' refers to those standards agreed and published by experts either internationally or nationally by independent, non-governmental organizations in order to ensure that certain requirements are met. Examples of standards organizations are the International Organization for Standardization (ISO), Underwriters Laboratories (UL), American National Standards Institute (ANSI), the European Committee for Standardization (CEN) and the Federal Agency on Technical Regulating and Metrology (ROSSTANDART).

seal (as barriers to entry); an audit of the security related business practices of the manufacturer; and a test of the seal's ability to indicate evidence of tampering.

5.10. Mechanical seals should withstand harsh environmental conditions, weather and chemicals. They should be resistant to tampering, should be easy to apply and seal and should be permanently and uniquely marked and numbered.

5.11. Combined seal and lock devices incorporate both a seal and locking functionality, enabling such a device to serve as both detection and delay measures for the package on which it is secured. The simple form of these systems involves a locking mechanism with a hole bored through the lock that allows a passive seal to be attached.

5.12. Passive seals indicate if the door or package that has been sealed with them has been tampered with or broken. These seals can be used to ensure that critical communications and operational components are not tampered with. Different types of passive seals (e.g. wired, plastic, tamper proof labels) can be used on the container directly as well as on the freight container or truck doors to detect any opening of the container or doors of the freight container or truck during transport. Examples of security and high security seals include bolt, cable or electronic seals. All seals should be numbered and have a unique identification so that they are not easily duplicated.

5.13. Electronic seals combine the properties of mechanical seals with an electronic capability to measure the integrity, store data and provide a communication signal. For example, such devices can use infrared signals, radio frequency identification (RFID) and other wireless protocols for communications. These seals can be either passive, which need a person or device to query the system to gain information on its status, or they can be active by collecting, processing and transmitting information actively to the operator or a transport control centre as appropriate.

5.14. Most types of electronic seals are able to automate seal verification and reporting and record events like opening and closing. In some systems, electronic seals also alarm if they are tampered with or if the seal component is broken. In addition, electronic seal systems are designed to be reusable, which offers a benefit over mechanical seals. Additional functionality includes the ability for authentication, security, tracking, alarm annunciation and automatic data capture. However, electronic seals also have drawbacks in that they are expensive compared to simple mechanical seals, necessitate additional user training and may necessitate further computer security measures to assure their integrity owing to their susceptibility to cyber-attack [25]. Examples of electronic seals include radio frequency enabled door seals, radio frequency identification (RFID) electronic seals, radio frequency enabled package seals and cargo container anti-theft devices with tracking systems.

5.15. The use of radio frequency door or package seals that securely transmit to an appropriate detection system could be considered for enhanced door or package security. Such seals can be used to accelerate the assessment of an intrusion attempt.

Tracking system

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

5.17. Many tracking systems are commercially available and can be used regardless of the mode of transport. The selected tracking system should incorporate features that secure and authenticate transmitted location information, provide local hardening against cyber-attacks [25] and operate without any action by the driver. Reports to the transport control centre can be event-driven, on demand, or scheduled.

5.18. It should be decided whether package or conveyance tracking will be used to maintain knowledge of the location of the package and/or the conveyance. One example of position tracking appropriate for some packages is bar code scanning at each transfer point.

Intrusion detection

5.19. In addition to visual observation, an effective means of intrusion detection may be used to provide an alarm if there is an unauthorized access to the material transport vehicle. An audible and/or visual indicator exterior to the conveyance should be used to indicate a breach of the cargo compartment. Such a system necessitates means to visually assess the alarm, such as monitors and the ability to send signals to the driver and other selected remote staff when attempted intrusion into the vehicle is detected. If applicable, these remote staff may be the escort, response forces and transport control centre. Mobile on-person and fixed in-cab driver duress buttons and remote communication systems provide means of communicating alarms from an access control or intrusion detection device. Examples of access control and intrusion detection devices include the following:

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

Locks, barriers and other delay measures

5.20. All packages should be secured to the cargo bed. If the material is transported in an open conveyance, the package should also be covered with a heavy-duty, waterproof cover such as a tarpaulin so the load is not open and viewable to the public.

5.21. Passive delay measures include items such as locks, lock shrouds, other locking mechanisms, secure tie downs, chains, cable nets, reinforced hinges, ballistic glass, armoured plates, tailgate lifts, containers, cages, and overpacks and secure tie downs with locks, cable nets, chains. In addition, passive delay measures include specific operational procedures, such as key control (see para. 5.46). Passive delay measures are most commonly installed in the cargo compartment and on the cargo itself, including the package.

5.22. High security locks with shielded shackle can be used for freight container doors and on the container, depending on the configuration. High security locks may prevent or delay attacks using hand held tools.

5.23. For most shipments, material is shipped in standard commercial cargo conveyances or shipping containers. Even for standard commercial conveyances, inexpensive and easy upgrades can enhance the security of the material, such as the use of high strength locks, lock shrouds and heavy-duty chains. Generally, the package is fixed to the vehicle bed using strong chains, nuts, bolts, ratcheting and related devices.

5.24. For sensitive shipments, special vehicles or specific transport security system upgrades may be designed and built to provide adequate delay. For example, the vehicle's load-carrying compartment can incorporate panels of multi-layer steel armour, thermal insulation, inner and outer steel skins and other barrier materials built on a steel frame. The armour combined with the overall thickness of the wall panels can provide both access delay and ballistic protection for the cargo.

5.25. The load-carrying compartment should be designed to accommodate not only the anticipated packages to be shipped, but also the associated transport security system to be used. The vehicle capacity is dependent upon the truck chassis selected for the cargo and the crew compartment, so decisions to armour one or both sections of the vehicle should be based on the load capacity of the chassis. Aircraft-type cargo tie-down tracks can be provided in the vault floor and perhaps on the vault sidewalls and roof. This arrangement allows flexible cargo tie-down schemes for containers, palletized loads or sidewall racks.

5.26. The use of an access control system that requires two-person controls and/or biometric or multi-factor verification can be installed to control access to the cargo area. An electromechanical locking system can be used to support these types of access controls.

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

5.28. If stand-off attacks in which an adversary seeks to create an explosive release of material are part of a threat assessment or the State's design basis threat, the cargo compartment of the conveyance should be designed to mitigate this type of attack, such as stand-off or multiple physical barriers. In addition to taking advantage of ballistic protection, thermal insulation, overpacks and radiation protection shielding, other design features may be needed to counter such an attack.

5.29. Vault construction can include multiple layers of blast resistant material. Rather than having a single thickness of material, the separation of multiple layers with other materials, even air gaps, has been demonstrated to provide enhanced ballistic and explosive protection. Thermal insulation, which is also fire retardant, can also be used to reduce the after effects of a stand-off explosive attack.

5.30. The package in which the material is transported can also contribute to the security of the material. Packages, such as Type B packages [14], which are designed to remain intact during transport accidents can provide protection against certain sabotage attempts.

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

(a) Ability to be loaded and unloaded without removal from the transport vehicle;
(b) Multi-layer wall structure;
(c) Visual decoys, such as non-operational bolts and keys;
(d) Ability for the overpack to be fastened to the vehicle from the inside of the overpack;
(e) Foam inner core in innermost wall for thermal protection;
(f) Double locking mechanical keys for opening and closing the overpack;
(g) Launching of a signal beacon following the unexpected opening of the overpack;
(h) Provision of GPS alert and confirmation upon arrival of destination;
(i) GPS tracking capabilities.

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

5.33. Conveyances specifically designed to resist stand-off attack and increase the likelihood of survival of the guards and transport crew should be equipped with the following:

(a) Bullet proof tires that are reinforced with Kevlar and shred and puncture resistant, with steel rims underneath the tires that can enable the vehicle to escape at speed even if the tires are blasted away;
(b) Protection for the petrol tank, such as armour plating and use of a specially designed foam tank which prevents it from exploding even if a direct hit is received;
(c) A reinforced steel plate under the vehicle for protection in the event of an explosive being placed underneath;
(d) Armour plating to protect the engine;
(e) Grille guards and bull bars made of heavy-duty steel and mounted to the front of the conveyance to protect the vehicle occupants in the event of a collision and to allow the conveyance vehicle to be driven off road through brush, debris and other obstacles in case of ambush.

5.34. Specific examples of these types of measure also include ballistic barriers, such as ballistic windows strong enough to withstand bullets or deflect explosive effects; armour plated doors; anti-carjacking devices such as additional locks on the doors; and discreet driver duress buttons.

5.35. Active delay systems can also be considered for use when designing a transport security system for sensitive shipments. Active delays can be divided into three broad categories – dispensable barriers, obscurants and vehicle operational control – which can be used to meet different security objectives. For example, if the security objective is such that any loss is totally unacceptable (e.g. for Category I nuclear material) or if the conveyance is going to be operating a significant distance from a timely response, active delay systems may be used to substantially increase the delay time.

5.36. Dispensable systems, when triggered, dispense a material that creates a barrier preventing access to the package or the material. These systems can be triggered manually either by the transport crew or transport control centre if unauthorized access is detected, or they can be triggered automatically by the actions of the adversary if they penetrate a boundary defined around the package. Examples of dispensable delays include sticky foam and tangle wire.

5.37. Obscurants, when triggered and released, create an intolerable or difficult work environment which the adversary must overcome in order to complete their tasks. Obscurants can include the use of cold smoke in order to create a blackout situation or the use of loud alarms or bright strobe lights in order to create a challenging environment for the adversary to complete their tasks.

Immobilization systems

5.38. Vehicle operational control systems can be used as part of the transport security system and are available in two forms: a vehicle authorization system and vehicle disablement or immobilization system. In either case, both systems should be protected from physical tampering and cyber-attack [25].

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

5.40. An immobilization system when activated shuts the vehicle's operating capabilities. These features can be incorporated into the vehicle that can be activated either from the vehicle or remotely. Remote activation could be performed either from one of the escort vehicles or by the transport control centre. The immobilization system may be reversible either by a variable timer or by manual resets.

5.41. Immobilization features include the following:

(a) Engine fuel shutoff devices: The electronic system disables the fuel pump or the fuel supply system.
(b) Turbo air shutoff valves: Prevents air from entering the engine for combustion.
(c) Accelerator linkage disablement devices: Electronically prevents the accelerator from increasing where the vehicle's on-board computer control systems slow the vehicle or prevent acceleration.
(d) Force controlled braking of the vehicle to bring it to a stop within a pre-determined time after initiation: Controlled braking of the vehicle could be accomplished by engaging the vehicles brakes slowly or at intervals so as to allow the driver to always maintain control.
(e) Brake engagement system: Causes the brakes to lock. This should only be used when the vehicle is stationary due to safety considerations.

Administrative measures

5.42. All personnel who are involved with the shipment should hold verifiable documentation, including photo identification, certificates and operating documents where applicable; and any necessary work permits.

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

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

(a) Are simple to understand and if need be written.
(b) Explain the roles and responsibilities of the personnel.
(c) Detail the following:
i. The expected security practices and precautions to ensure the safety and security of the personnel as well as that of the cargo;
ii. The actions of the personnel before and during the shipment, upon departure and during and following delivery;
iii. The actions of the personnel during planned stops (e.g. fuelling breaks or driver relief) and unplanned stops;
iv. The actions and responsibilities of the personnel during unexpected events or emergencies.

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

5.46. Introduction of a two-person rule is a good practice to reduce the insider threat during transport whenever practical [33]. One way to implement the two-person rule is to provide two different keys for the radioactive material container and freight container locks to two different people. Additionally, the cargo area may be locked with more than one lock and the keys for each lock distributed among different people [2]. If the conveyance is under escort, one unique set of keys may be given to the escort team and one unique set to the driver. Keys to critical locks may be sent to the receiver of the shipment or travel separately from the shipment. The same approach may be implemented when employing other forms of locking mechanisms, such as key card readers or biometric scanners.

5.47. The vehicle should never be left unattended. A two-driver rule helps to assure this since one will always remain, awake and alert, in the vehicle at all times. If, however, the vehicle is left unattended for a short period of time, the vehicle needs to be kept under lock with alarm activation and immobilized (see paras. 5.38–5.41). It is a good practice to park the vehicle in well-lit and secure areas which are continuously under surveillance by security guards or law enforcement. When a security guard is not available to provide surveillance of the vehicle, the driver and/or other transport personnel can provide surveillance where applicable and in accordance with the regulations and/or approve the transport security plan.

5.48. In case of a technical breakdown of the vehicle, the carrier should have arrangements in place to provide repair or to tow the conveyance to a repair facility. Carriers should have a plan to move an inoperable cargo vehicle with its nuclear or other radioactive material cargo to the nearest secure location where compensatory security measures can be applied until the repair or replacement of the

vehicle is complete. If this is not possible, there should be contingency measures in place to create a temporary secured area around the vehicle (e.g. deployment of additional escort forces).

5.49. To be prepared for incapacitation of drivers, carriers should designate backup drivers in advance and include them in the convoy. If the convoy stops because of driver's incapacitation, the escort unit should take measures to ensure safety and security such as directing traffic while protecting the convoy.

5.50. A convoy commander should be assigned for each road convoy who has responsibility for relaying information and instructions to and from the crews of each vehicle. The convoy commander is responsible for the safe and secure conduct of the shipment. This person should be the primary contact between the shipment and the transport control centre. Subordinate leaders, such as an escort commander, could be assigned amongst the guards present in the escort vehicles.

5.51. The transport security plan, where appropriate, should detail the size and structure of a convoy, such as the number of conveyances per convoy and the number of escort vehicles per conveyance, spacing between escorts vehicles and conveyances of convoy and limits on the number of vehicles parked at the same stopover site.

5.52. During a shipment, the convoy commander and guards should be responsible for taking all immediate reactive measures. In the event of an attempted sabotage the convoy should make best effort to keep moving, to get the cargo to a secure location. If one of the conveyances is disabled, the other conveyances within the convoy may need to move and park at a safe and secure location to avoid additional exposure to the attack. This will involve dividing the escort force and should be done in accordance with the contingency plan. Information should be centralized with the convoy commander and shared with the transport control centre and, when appropriate, law enforcement.

5.53. The necessity of route changes should be assessed along with law enforcement and should be communicated with the transport control centre.

TRANSPORT SECURITY MEASURES RELATING TO ESCORT OF SHIPMENTS

5.54. Escorts are armed or unarmed personnel trained and equipped to protect the shipment. These personnel travel either in the transport conveyance or accompanying vehicles. These personnel and vehicles should be appropriately equipped to communicate with the transport control centre or external response organizations.

5.55. The designers of transport security systems should determine the level of protection and armament for the guards based on the threat assessment, the tactics that the guards should be expected to use and the use of force allowed by the State. If national regulations require that a shipment utilize armed guards, those guards should be equipped with weapons in line with the State’s legal requirements and should also be provided with personal protective and communications equipment. If guards are to be armed,

the next consideration is the selection of the weapons. Examples of what might be considered, as allowed by the State, include: side arms (handguns), long guns (rifles), automatic and semi-automatic weapons, hand grenades, indirect fire munitions, batons, tasers, pepper spray or other chemical irritants, smoke grenades and flash bangs.

5.56. During the process of determining how guards are to be armed, guidance and procedures should also be developed and training provided regarding the conditions under which guards are permitted to employ their weapons, in accordance with the State's laws.

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

5.58. Consideration should be given to protecting not only the material, but also the personnel of both the transport conveyance and the guards (also referred to as the internal response force) to increase the likelihood of survival of the guard force and transport crews in the event of an attack. If a shipment is attacked, not only can guards and other transport personnel provide detection, but they also can, if properly equipped, delay the adversary from accomplishing their task. The guards and transport crew need to be able to communicate a duress signal. This may be accomplished with a mobile on-person or fixed in-vehicle duress button, intended to keep the conveyance moving if possible, to activate other security measures and to actively participate in the protection of the shipment.

5.59. Moreover, if the number of guards accompanying the conveyance and surviving the initial stages of an attack is large, the need for other delay measures is reduced as the guards can provide delay. Conversely, if this number is small (either due to high casualties or due to a small initial number of guards), a greatly increased delay time needs to be established in order to allow the remaining guards sufficient time to redeploy to defend the cargo. If the shipment is travelling in remote areas of the route where sizeable secondary response forces are not available immediately, the guards play a valuable role in protecting the material. Therefore, it is important that their survivability is enhanced. In addition, the transport crew should be able to maintain control of the conveyance and prevent the adversary from using the conveyance to escape with the material.

5.60. Increasing the likelihood of survival of the guards and transport crew in case of an attack should be considered in the design stage. Typically, building in the needed protection will add considerable weight to the chassis and the gross weight of the chassis should be considered, both empty and with the largest expected package to be transported. An appropriately sized chassis will be critical to ensure the vehicle functions as designed.

5.61. Accompanying guards should continuously observe the vehicle and surroundings. Typically, transport crews, guards or escorts will be the first to assess and validate an alarm that is initiated from

the conveyance. Consideration may also be given to employing a lead reconnaissance vehicle that travels in advance of the shipment to visually assess route situations, raise alarms as needed, possibly redirect the shipment and initiate response force actions as needed.

5.62. For shipments by rail, escorts and/or guards should accompany the shipment to maintain surveillance of the rail freight car or freight containers containing nuclear and other radioactive material by travelling in an adjoining guard car and/or using closed circuit cameras.

TRANSPORT SECURITY MEASURES RELATING TO THE TRANSPORT CONTROL CENTRE

5.63. The transport control centre is an integral element of the transport security system, as it serves as a communication and tracking hub. Use of a transport control centre is recommended for transports of nuclear material in Category I and II, and of radioactive material as an additional security measure. Even if a transport control centre is not used as part of the protection strategy, every shipment should have a single point of contact for the driver or escort personnel to call in the event they need assistance.

Technical measures

5.64. The transport control centre should be protected against a threat aimed at influencing or neutralizing its role. Both physical protection systems and computer security programmes and measures [25], consistent with national strategies, should be in place to protect the transport control centre from the current threat as defined in the threat assessment or design basis threat. Physical and cyber access to the transport control centre should be limited to authorized personnel only and measures to prevent unauthorized access should be established and maintained via intrusion detection systems. The transport control centre should also use redundant, diverse and secure communication channels and should be equipped with emergency electrical power.

5.65. Under normal operation, where needed, the transport control centre should have the ability to constantly monitor the shipment. This can be done through GPS tracking or through established reporting at intervals by the transport personnel. The transport control centre should also track the current position and security status of the shipment of material, alerting response forces in case of an attack and maintaining continuous secure two-way voice communication and text communications with the shipment and the response forces.

5.66. The State’s competent authority may have their own transport control centre. In this case, the State should arrange communication relationships as well as security requirements for the information and digital assets communicating between the State’s transport control centre, operator’s transport control centre and the shipment. Regardless of the operator of the transport control centre, consideration should be given to appropriate level of staffing, operating hours and staff training, to ensure proper and effective coverage.

5.67. For maritime transport, the transport control centre should be located in the flag State of the ship and staffed at all times during the shipment by properly trained and vetted personnel. The ship should be equipped with a system which enables the transport control centre to monitor its location at regular intervals and upon request.

Administrative measures

5.68. A formal transport control centre consists primarily of a central point of contact and monitoring of the shipment. The personnel that operate the transport control centre should have all necessary information pertaining to the transport, such as: the material being shipped; the different shipping actors (e.g. shipper, carrier, receiver, freight forwarders); any in-transit points and organizations (e.g. ports, airfields); and information for initiating the contingency and response plans, as needed.

5.69. If a nuclear security event occurs during the shipment, the transport control centre should have information on whom to contact and when as well as which critical information is needed to be conveyed. This should be formalized in the contingency and response plans.

5.70. Transport control centre personnel should be able to advise the driver while the shipment is on route, for example in case of a severe accident, a demonstration or road closures along the scheduled route that might have security implications.

5.71. The transport control centre should have priority for contacts with the convoy commander as well as with all other involved parties. A clear chain of command should be established with the correct contact information associated to all members. This chain of command and the communication arrangements should be provided to the transport control centre, the driver of the shipment, the convoy commander and their subordinate leaders.

COMMUNICATIONS IN TRANSPORT SECURITY SYSTEMS

5.72. The ability to have two-way communication systems throughout the shipment is critical. There are two significant types of communications: administrative and operational.

5.73. The administrative communication covers the communication that occurs during the planning and closeout phases. It includes submission of transport documents, including the transport security plan for regulatory review and approval. It also includes pre- and post-shipment notifications between shipper, receiver, other third-party entities (e.g., customs, carriers, operators) and the competent authority. It should be ensured by all stakeholders, that this information is transmitted and managed in such a way as to limit distribution to only those that have a need-to-know.

5.74. Operational communication covers all forms of communications during the conduct of the transport to include intra-shipments communications as well as communications between the shipment, its escorts and the transport control centre. This may be in the form of either data and/or voice. A subset

of the operational communication deals with communications during a security event between the shipment and the external response forces. This form of communication is typically done via cell phone and can be intercepted. This needs to be understood by those using those communication tools so they guard against transmitting sensitive material.

5.75. There are several operational considerations that should be planned for when developing the communication structure. Most importantly, the communication system should function throughout the entire route. These communications might employ different platforms (e.g. cellular, radio or satellite) and methodologies (e.g. voice or data). Some examples of communication technologies include secure encrypted handheld communicators, satellite-based communications equipment and mobile or handheld general frequency receivers and transceivers, such as very high frequency (VHF) and ultra-high frequency (UHF). If possible, these communications systems should be encrypted to prevent the general public and adversaries from monitoring communications within the transport system. If open communications must be used, techniques such as code words and phrases should be considered to provide some protection for sensitive information that needs to be communicated.

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

5.77. Provision for communication capability is important for timely reporting of any security event to initiate a response, as appropriate. Therefore, means of communication such as cell phones, two-way radio, computers, radios, satellite phones with voice and text messaging should be provided to drivers, escorts and other transport crew. Redundant means of communication may be considered if the transport is undertaken in remote areas where the lack of infrastructure necessitates the use of multiple technologies. This also helps ensure maintaining the communications capability in case one device fails. It is important to note that as well as other standard communication systems, GPS signal, duress button(s) and their corresponding alarms need to be tested prior to departure of the shipment from the shipping facility.

5.78. Special verbal duress codes should be established and kept confidential prior to each trip. In addition, special passwords can be pre-established so the carrier can verify they are only speaking with the assigned drivers.

5.79. Drivers and other transport personnel should be given written instructions to be used in case of a security related event. The instructions should include, among others, location of authorized stops, operation of alarm systems, actions to be taken in case of theft or sabotage of the vehicle or package, phone numbers of key personnel of the operator and law enforcement.

TRAINING AND QUALIFICATION OF THE TRANSPORT SECURITY PERSONNEL

5.80. Security awareness training is required in dangerous goods transport safety regulations such as the UN Model Regulations [5], those issued by the International Maritime Organization [6], and International Civil Aviation Organization [7] and in most regional agreements which refer to these documents. Training used to satisfy the requirements for the transport of dangerous goods may also be used for the transport of nuclear and other radioactive material, since these materials belong to Class 7 in the dangerous goods regulations. Security awareness training may also be integrated into existing mandatory safety training and could be delivered through different means, such as online or web-based training or in-person training. Any specific security concerns relating to the potential radiological consequences resulting from the nuclear and/or radioactive nature of the material should be emphasized in the training.

5.81. All persons engaged in the transport of dangerous goods should have basic security awareness training. Basic security awareness training includes understanding the need for transport security, the nature of security-related threats, methods to address security concerns and actions to be undertaken in the event of a security event. It should include awareness of transport security plans, contingency and response plans when appropriate, commensurate with the responsibilities of individuals and their roles in implementing these plans.

5.82. Such training should be provided or verified upon employment for all personnel involved in the transport of nuclear and other radioactive material and should be periodically supplemented by refresher training at intervals as required or deemed appropriate by the competent authority or the operator's employer.

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

5.84. Some international organizations and government agencies have published training course development guidelines that may be helpful in identifying the type of security training appropriate for various job responsibilities and the recommended content of this training.

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

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

5.87. Non-security personnel might also be assigned duties and responsibilities relating to the security of the material. In this case, these personnel:

(a) Should be trained, qualified and periodically re-qualified to perform assigned duties through established training programmes;
(b) Should be provided with the necessary equipment to perform their assigned duties;
(c) Should possess the knowledge, skills and abilities, including physical attributes such as sight and hearing, needed to perform their assigned duties and responsibilities.

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

5.89. The training should also include radiation safety and protection awareness, training on security threats and risks related to the material being transported, type of packages and activity permitted in each package, response plans and communications.

6. DEVELOPING, IMPLEMENTING AND EVALUATING A TRANSPORT SECURITY PLAN

6.1. The competent authority should request that a transport security plan be prepared for Category I and II nuclear material as recommended in Ref. [11] and for radioactive material which is assigned to the enhanced transport security level as recommended in Ref. [12]. The transport security plan may be requested as the competent authority deems necessary for Category III and below nuclear material and other radioactive material on the basis of the level of threat or the relative attractiveness of the material.

6.2. In this section, the process of developing, implementing and evaluating a transport security plan is described, including examples of good practices. This section also provides guidance on the content

of a transport security and how to effectively implement and maintain the plan as part of the transport security system.[5]

PREPARATION OF A TRANSPORT SECURITY PLAN

6.3. The competent authority should provide the shipper or carrier with clear expectations for the content and structure of the transport security plan as well as clearly defined specific requirements and guidance on its proper preparation and implementation. Based on this information the shipper or carrier should develop a transport security plan, incorporating a range of security measures and following the completion of a vulnerability assessment and the design of a transport security system, as described in Sections 4 and 5. Appendix I of Ref. [11] provides a sample transport security plan for nuclear material and Appendix II of Ref. [12] provides a sample transport security plan for other radioactive material. A given transport security plan may address single or multiple similar shipments and may be valid for a specified period of time or number of shipments.

6.4. If the shipper or carrier uses a subcontracted carrier or freight forwarder, the shipper or carrier should ensure that these meet the requirements of the transport security plan, implement a mechanism to verify these measures and retain records. Additionally, contractors and their employees involved in the transport of nuclear or other radioactive material should undergo the same pre-employment screening process as new employees of the operator. Responsibility for implementing these checks should rest with the contractor, and the operator should request from the contractor to demonstrate, from their records, that they have carried out these checks.

6.5. If the shipper or carrier maintains the same transport security plan across multiple shipments, then they should, in accordance with regulatory requirements as applicable, review the transport security plan regularly and update it as needed. The transport security plan should also be updated if any significant changes are made to the transport security system, if the threat changes, if processes described in the plan change or if regulatory changes mandate an update. The competent authority may request re-submission of the plan at defined intervals from the shipper or carrier for review and/or approval in case of already approved campaigns of shipments where this transport security plan is applied.

6.6. A transport security plan may be prepared along the following steps:

(1) Step 1: The shipper or carrier designates an individual with overall responsibility for the transport security plan, who could either be tasked with oversight of a drafting team or given the responsibility to draft and complete the transport security plan.

(2) Step 2: A team of individuals with responsibilities under the plan is selected. For example, the team might include a radiation safety officer, a security specialist and a logistics specialist. The

[5] The IAEA has developed an example transport security plan available to Member States upon request.

size of the team should be as large as needed to adequately address security requirements and may be as small as one person.

(3) Step 3: The next task should be to outline, plan and prepare the structure of the transport security plan. Considerations for developing a transport security plan are outlined in paras 6.7–6.32, in appendix II of Ref. [12] and in appendix I of Ref. [11].

(4) Step 4: Relevant data and information pertaining to the shipment should be gathered by the responsible individual and/or drafting team. When all needed information is collected, this information should be used to develop a draft transport security plan.

(5) Step 5: The draft transport security plan should be approved by the management of the shipper or carrier.

(6) Step 6: The completed transport security plan approved by the shipper or carrier should be submitted to the regulatory authority, if required.

(7) Step 7: The competent authority should approve the transport security plan, if required, or might request additional information from the shipper or carrier developing the TSP in order to grant approval. If additional information is requested by the competent authority, then steps 4– should be repeated.

Considerations for developing a transport security plan

6.7. The shipper or carrier should develop the transport security plan, should obtain the necessary inputs from all relevant stakeholders (e.g. response forces or other competent authorities) and should submit the transport security plan for approval to the competent authority, as required.

6.8. Necessary inputs may include route information (e.g. primary and alternate routes, bridges and tunnels, planned events along the route, road conditions), material and vehicle description and the transport convoy composition. Further inputs may include security considerations of the shipment such as escorts (armed or unarmed), communications, and delay measures (e.g. vehicle immobilization devices).

6.9. Taken separately, information such as the quantity of the material, the date of the shipment and the route of the shipment might not be sensitive, but when this information is combined, the resulting document should be sensitive and should need to be adequately protected.

6.10. In the following subsections, a number of other types of information that should be considered for inclusion in the transport security plan are discussed in more detail: threat and vulnerability assessment, protection of information, planned and alternate routes, description of the conveyance, proposed security measures and communication arrangements.

Threat and vulnerability assessment

6.11. A transport security plan should address the relevant threats contained in the national threat assessment. The threat assessment should be conducted by the State in advance of the shipment. The shipper or carrier should consider additional security measures if the threat level is increased or could consider adjusting the routes, itinerary and timing of shipments in order to mitigate risk. More information on threat assessments can be found in Ref. [34].

6.12. The security system for a transport operation should be assessed to determine if there are unacceptable vulnerabilities to the shipment. This is typically done through a vulnerability assessment process, during which the transport security plan itself is reviewed and tested (see para. 4.26). The methodology used for performing the vulnerability assessment should be included in the transport security plan.

Protection of information

6.13. A transport security plan contains sensitive information such as schedule, routes, security measures and response capabilities that should be appropriately protected, in accordance with the national requirements for information security.

6.14. The transport security plan should only be distributed on a need-to-know basis and only to individuals with a valid trustworthiness verification through a background investigation process.

6.15. For information security purposes, the transport security plan as a whole should be protected to the highest sensitivity of the information contained within it. The transport security plan may be divided into more than one document or separate sections may be developed for the purpose of transmitting information on a need-to-know basis. This practice can ensure that those persons with responsibilities under the transport security plan only have access to the information that is necessary for the performance of their duties. For example, in most cases, vulnerability assessments associated with the shipment would be highly protected and should have a well-controlled, limited distribution. A shipper may choose to keep the vulnerability assessment separate from the rest of the transport security plan in order to protect the sensitive information contained in it when distributing other, less-sensitive sections.

6.16. Submission of the transport security plan and any accompanying documents to the competent authority would be in accordance with information security controls required by the regulatory body, including transmission by encrypted e-mail, fax, secure courier, or hand delivery. Ref. [24] provides more information on these topics.

Planned and alternate routes

6.17. When selecting the planned or alternate routes for the transport of nuclear or other radioactive material, the shipper or carrier should consider applicable regulations and ordinances regarding the

transport routes for hazardous materials and especially take account of any regulatory restrictions placed upon the type of material being transported.

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

6.19. The shipper or carrier may also make route selections based on safety and security considerations. For example, when choosing routes for the shipment, the shipper or carrier should consider road conditions, response times along the route, communication capabilities and permissible speed, as well as potential hazards such as rockslides, floods, snowstorms or forest fires that could adversely affect the shipment. Additional factors to consider include, where practical, avoiding heavily populated or urban areas, selecting routes where response elements can effectively respond and minimizing constricting infrastructure such as bridges and tunnels. The shipper or carrier drafting the transport security plan should consider these issues, avoid potential hazards if possible and, if not, have a plan to deal with related complications that might arise. For example, if the route has to transit an urban area, the transport security plan may include a description of the precise route to be taken through the area and how the shipment is to be scheduled to avoid times of peak traffic. If transfer points, temporary storage areas, stopover facilities, safe havens, or subsistence locations are included in the planned or alternate routes, the transport security plan may reference other security plans for these locations.

6.20. Furthermore, route variability to avoid creating patterns, such as using the same route and shipping at the same time of day for every shipment, can provide significant protection and make it more difficult for an adversary to plan an attack. For similar shipments (e.g. transporting the same type of nuclear or radioactive material, using the same conveyance, or the same origin and destination), variability can increase unpredictability and provide significant protection to the shipments. Changing shipping patterns, such as routes and timing of shipments, can make it more difficult for an adversary to plan and initiate an attack.

6.21. As the first step of planning a route, online mapping applications, satellite imagery and aerial photography may be used. However, these sources only offer a limited amount of information on the conditions of the chosen route. Therefore, the shipper or carrier planning the route may consult with relevant authorities to request accurate information or may conduct their own reconnaissance of planned and alternate routes to ensure that route conditions are appropriate for the shipment. For example, subjects of interest during route reconnaissance may be the conditions of roads, presence of railways

and crossings, tunnels or bridges, the road width, the gradient of the road, repair or construction work that is being, or is expected to be, performed, as well as the locations, conditions and fuel supplies of refuelling sites.

Description of the conveyance

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

6.23. If the proposed shipment involves intermodal transport and/or intermodal transfers of the material, the details of the conveyances should be provided separately in the transport security plan for each mode. For example, this might occur if the shipment is transported by road to a rail terminal, loaded onto a railcar, then transported by rail to an airport, loaded onto a plane, transported by air, loaded onto a truck and finally transported again by road to the planned destination site. The details provided in the transport security plan should include the date, time and location of the planned transfers, any planned temporary storage throughout the shipment and the names of the convoy commanders for each mode of transport.

Proposed security measures

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

Communication arrangements

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

6.26. In addition, communication arrangements to be used within and between each unit or organization involved in the shipment should be described, including the specific communications methods to be used. These may include communication arrangements with:

(a) The shipper;
(b) The carrier transporting the material;
(c) The receiver of the material;
(d) Any response forces located along the transport route;
(e) Any transport control centre that is to be established for the operation.

Arrangements with response forces

6.27. The transport security plan should also include descriptions of the arrangements between the shipper or carrier and any potential response forces located along the transport route. The proposed arrangements should include provisions for establishing effective communications with any response forces along the transport route.

6.28. Arrangements should take account of the different jurisdictions and agencies that have response responsibilities along the route of the shipment. Accordingly, all changes in the proposed communications methods or protocols for communicating with various response forces that should occur along a transport route – such as changes in radio frequencies or radio or cellular encryption methods – should be clearly described in the transport security plan. The methods of communications with various agencies and the jurisdictional and operational boundaries occurring along the route should be verified to be accurate by the shipper or carrier.

6.29. In addition to the communication arrangements, any special security arrangements to be made with response forces, including those required by the regulatory authority for a given shipment, should also be set out in the transport security plan. For example, a response force, such as law enforcement or a private security firm, may provide an armed escort for a shipment of material. Where special security arrangements involve more than one response force, such as movement from one jurisdiction to another or across an international border, the plan should describe the cooperative arrangements for transferring responsibility from one response force to another. The plan should also describe any coordination arrangements between members of the response force and those personnel involved in the logistical aspects of the shipment such as the driver or escorts.

Contingency planning

6.30. The shipper or carrier should have in place contingency plans and response plans to detail pre-planned responses to different postulated scenarios, including those of low probability abnormal events that might impact the security of a shipment. The number and type of scenario that need to be covered

may be prescribed by the competent authority or the operator might have to determine what is appropriate.

6.31. Situations during transport that may be addressed with contingency plans and response plans, as appropriate, include various abnormal events and accidents, for example as follows:

(a) Technical breakdown of the conveyance or escort vehicles;
(b) Incapacitation of the driver or other convoy personnel;
(c) Delayed or stopped convoy;
(d) Route changes;
(e) Route deviation;
(f) Malfunction of tracking systems, communications, or other equipment;
(g) Traffic accidents
(h) Natural disasters;
(i) Attacks on the shipment such as attempted sabotage and unauthorized removal, (e.g. disabled cargo vehicle).

6.32. A prescribed and pre-established route, agreed upon between the carrier, law enforcement and competent authorities is important to ensure any route changes and possible deviations are approved and/or monitored to ensure the shipment remains secure. This also allows preclearance with other activities which may be taking place along the route (e.g. construction, road maintenance, special events).

6.33. In contingency planning it is important to prepare for any time the convoy might change the route or deviate from its planned route. In this respect, route changes are typically made due to new information that a threat is imminent. The convoy should proceed to an alternate, pre-approved route. Route deviations, on the other hand, are typically made due to unforeseen barriers that are not directly threat-related, such as a fallen tree blocking the current route or a major accident blocking the roadway ahead where passage is impossible or unrealistic for an extended period of time making deviation necessary. The convoy should take an immediate detour to bypass the barrier and then return to its prescribed route as soon as is practical.

APPROVAL OF A TRANSPORT SECURITY PLAN BY THE COMPETENT AUTHORITY

6.34. If the competent authority chooses to require that the transport security plan be approved prior to the commencement of the shipment, the competent authority may choose to integrate this requirement into the licensing and authorization process for transport of nuclear and other radioactive material. If such a regulatory requirement is in force, it should be communicated to the shipper and carrier to facilitate timely submission of transport security plans and to allow the competent authority sufficient

time to conduct their technical assessment of the transport security plan for completeness, adequacy and, if required, approval.

6.35. The review of the transport security plan is performed by the competent authority and should be based on the national requirements for the security of nuclear or other radioactive material in transport (e.g. existing national regulations), the design basis threat or any representative threat statement, the vulnerability statement, if required, and other regulatory documents. For the approval of the transport security plan, the competent authority may involve the input of relevant stakeholders.

EVALUATION OF A TRANSPORT SECURITY PLAN

6.36. A good practice is to evaluate the transport security plan or elements listed in the transport security plan before a shipment to assess its effectiveness. For example, the transport security plan can be evaluated through facilitated discussion, table-top exercises, drills or limited or full scope exercises. Ref. [32] provides information on the preparation, conduct and evaluation of exercises for the security of nuclear and other radioactive material in transport. These exercises may involve a range of stakeholders such as law enforcement or other competent authorities that have responsibilities related to the transport security plan. Following this evaluation, it is a good practice to capture the identified lessons in an after-action report and to adjust the transport security plan as needed. The validity of the transport security plan should also be evaluated in light of new or changing threat environment or transport conditions. Resulting adjustments of the transport security plan may be submitted to the regulatory authority for approval, if required.

6.37. Another good practice is to evaluate events or other deviations from the transport security plan that occurred during previous shipments and identify any resulting necessary improvements of the transport security plan. Based on this information, the TSP should be updated for future transports. This is particularly relevant for shipments where similar aspects (e.g. transporting the same kind of nuclear or radioactive material, using the same conveyance, or the same origin and destination) exist from shipment to shipment. The same transport security plan should not be used for other shipments without a prior evaluation to assess its validity and appropriateness to the specific shipment.

Compensatory measures

6.38. Situations might arise, where it might not be possible to implement some of the security measures required by the national requirements. For example, already approved security measures might malfunction during transport and replacement might not be feasible or reasonable. In this case, compensatory security measures can be implemented to provide a commensurate level of security.

6.39. Prior to implementing compensatory security measures, the shipper or carrier should conduct an analysis to determine whether the compensatory measures will provide a level of security that fulfils the national requirements. The details of the specific compensatory measures used should be documented

as evidence that adequate security is provided in a manner commensurate to that described in the transport security plan. The proposed compensatory measures should be submitted to the competent authority who should only approve the proposed compensatory measures when satisfied that they provide a commensurate level of protection. Otherwise, they should require improvements to the compensatory measures. Considerations on information security which were described for the transport security plan should also be valid here.

6.40. Compensatory measures need to be implemented prior to the commencement of the shipment to ensure that the capability to detect, assess, interdict and neutralize threats to the shipment are sufficiently maintained at all times and meet the national requirements.

6.41. Examples of compensatory measures include the following:

(a) A security escort can be used to provide a balanced system if the use of multiple physical barriers is not possible during transport.
(b) An intrusion detection system equipped on a conveyance or container or additional delay measures inside the conveyance, such as additional chains, lock bars or other delay devices, can be used if the use of multiple physical barriers is not possible during transport.
(c) A back-up means of communication and an alternate means of determining the location of the consignment can be used if there is a malfunction with the duress button; an issue with sending, transmitting, or receiving a GPS signal; and/or when the transport control centre cannot be reached directly.
(d) The escort can be used to communicate the status of the shipment vehicle to the transport control centre with a frequency that compensates for the lack of communication on the shipment vehicle itself if a key component of the communication system on the shipment vehicle has malfunctioned.

7. MAINTAINING SECURITY DURING TRANSPORT

7.1. There may be several phases of a transport operation and events for which continuity of security should be considered by the States involved as well as the shipper, carrier and receiver, such as:

(a) When a conveyance moves from one State into another;
(b) When a consignment is transferred from one carrier to another;
(c) When an intermodal transfer is undertaken;
(d) When a shipment is stored temporarily until it is accepted by another carrier and/or State (see (a)–(c));
(e) When unplanned stops occur;
(f) When the personnel involved in the transport changes;

(g) When security-related information is exchanged between States by electronic media or post;

(h) When an incident or accident occurs during transport, which may compromise the security arrangements;

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

(a) Security measures applied to the conveyance and at the intermodal transfer site, the temporary storage facility, or other location used during transfer from one carrier to another;

(b) Communications during transport;

(c) Tracking devices and their transmission of information by mobile communications network or satellite-based systems.

7.3. Mode-specific provisions and those relating to continuity of security for transport are covered in Ref. [11] and that guidance may extend beyond nuclear material to include transport of other radioactive material, where applicable.

INTERNATIONAL LEGAL INSTRUMENTS AND RECOMMENDATIONS FOR TRANSPORT SECURITY

7.4. International legal instruments are important in managing continuity of security, particularly across borders between States and when considering intermodal transfers.

7.5. Several international organizations address transport security for dangerous goods by the different modes of transport. These international organizations have developed legal instruments and recommendations for safety and security. In addition, these regulations, instruments and recommendations are often adopted by States for domestic transport. These legal instruments and recommendations are discussed in the paras 7.6–7.17.

Transport by sea

7.6. Under the auspices of the International Maritime Organization, international conventions and guidance provide information relating to the transport security of dangerous goods, including nuclear and other radioactive material in the maritime domain. Instruments pertinent to maritime security considerations are the Safety of Life at Sea (SOLAS) Convention [38] and three Annexes to SOLAS: the International Ship and Port Facility Security (ISPS) Code [38], the International Maritime Dangerous Goods (IMDG) Code [38] and the International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships (INF Code [38]).

International Maritime Dangerous Goods Code

7.7. Maritime shipments of nuclear and other radioactive material are subject to the IMDG Code [38]. This code requires that certain elements of security awareness relating to dangerous goods be included in training for crewmembers. Those crewmembers involved in shipments of these dangerous goods should be familiar with the provisions of relevant security plans commensurate with their responsibilities. The focus of the IMDG Code [37] is on the security of the material rather than maritime security elements such as vessels or port facilities.

7.8. Key provisions of the IMDG Code [37] reference existing international requirements and IAEA recommendations for transport security of nuclear material by sea. This ensures alignment between the IMDG Code requirements and those requirements and recommendations made in IAEA publications [38].

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

7.9. The IMDG Code also requires that certain shipments of nuclear material be transported on specially designed vessels, as specified in the INF Code [38]. INF cargo may only consist of packaged irradiated nuclear fuel, plutonium, and high-level radioactive waste. Further information on the classification of INF ships can be found in the INF Code [38].

7.10. Vessel classification in the INF Code is designated using a graded approach to certain safety features of the vessel design and on-board equipment, but these features are not related to nuclear security; however, they may support transport security overall. Transport security measures should be applied using a graded approach based on existing IAEA publications [38].

International Ship and Port Facility Security Code

7.11. The ISPS Code establishes security requirements and recommendations during maritime transport for vessels and port facilities, including personnel involved in these operations. These requirements and recommendations apply to international voyages for maritime transport and domestic short sea shipping within a State's jurisdictional limits.

7.12. The ISPS Code requires that a vessel security officer be assigned to each vessel during its voyage. The vessel security officer is responsible for maritime security of the vessel during its operation and is aware of all cargo onboard. When a transport security plan is drafted, it should be consistent with the content of the security plans provided by The ISPS Code and the vessel security officer should be consulted regarding its content and associated measures involved during the maritime leg of the voyage.

7.13. The ISPS Code requires a vessel security plan and a facility security plan (FSP). The vessel security plan and facility security plan may be referenced in or included into a transport security plan,

as appropriate. Both the vessel security plan and facility security plan may include additional requirements for monitoring and controlling access and activities of authorized persons on the vessel and port facility, including trustworthiness determination. Furthermore, the vessel security plan and facility security plan include security measures such as the availability of communications and associated systems.

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

Transport by air

7.15. The International Civil Aviation Organization, through the Chicago Convention, has published Annex 17 to the Convention on International Civil Aviation which addresses security of civil aviation, including security in airports [39].

7.16. The International Air Transport Association has also published a security manual that outlines principles to be used by commercial airlines to build effective aviation security measures [40].

7.17. Any general training in application of the International Civil Aviation Organization or International Air Transport Association security provisions should also be beneficial for understanding how effective security of nuclear and other radioactive material may be accomplished under these modes of transport.

SAFETY AND SECURITY INTERFACES DURING TRANSPORT

7.18. While, as stated in Ref [1], nuclear safety and nuclear security share the same goal, which is to protect people and the environment from harmful effects of ionizing radiation, the activities that address nuclear safety and nuclear security may be different, and sometimes actions taken to strengthen nuclear safety may affect nuclear security, either positively or negatively, and vice versa.

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

Management and administrative interfaces

7.20. As a shipper develops the plan to safely move material, it is best practice to also plan for its security during transport. Therefore, it is necessary to ensure that planning and coordination is organized among the different functional entities responsible for safety, emergency response, security and law enforcement that should comprise overall emergency response efforts.

7.21. In certain circumstances, information requirements associated with security and safety may conflict, notably when sharing information relating to the operational aspects of a shipment, such as with a transport security plan, or with the authorization, such as with a transport licence application. For safety reasons and often for regulatory compliance, various stakeholders may receive information about the shipment, such as the type of the material being transported, the day of departure and the shipment's planned route, so that government agencies with jurisdiction over the shipment (e.g. licensing) or along the route (e.g. escorting) can properly plan and support the shipment. However, for security purposes, sharing of this information should only be on a need-to-know basis and done in such a way that protects the information from those that do not need to know. The shipper and competent authorities should apply a risk informed approach to handling and transmitting need-to-know information. They should also assess what information needs to be shared, to whom it should be shared and when and how it should be shared so that it does not present a security risk but still meets all national safety requirements.

7.22. Other examples of areas where the interfaces between safety measures and security measures might need to be managed are the following:

(a) Safety and security inspections;
(b) Design of transport packages (addressed in para. 7.24);
(c) In-transit storage;
(d) Communication;
(e) Written instructions and documentation;
(f) Marking and labelling of packages and placarding of vehicles and freight containers;
(g) Development and implementation of compensatory measures.

7.23. These interfaces and possible ways to address challenges in the management of the safety–security interfaces are described in Ref. [13] for commercial shipments of radioactive material. The given information may in principle also be valid for a broader range of nuclear and other radioactive material in transport and may be applied accordingly.

Packaging

7.24. For all shipments of radioactive material, the UN Model Regulations [5], using the requirements originally stated in SSR-6 (Rev. 1) [14], establish design requirements for transport packages following a graded approach. For normal commercial shipments of radioactive material, these packages could

include excepted packages with the least robust design, industrial and Type A packages of moderately robust design or Type B packages with the most robust design.

7.25. There are cases where the robustness of the package design, for safety purposes, may also provide security benefits during transport.

7.26. Type B packages used for transporting large quantities and high activities of irradiated materials are often large and massive. For example, a Type B package for spent irradiated nuclear fuel may weigh up to 130 tonnes. Their large mass makes unauthorized removal from the transport conveyance extremely complicated, necessitating the use of specialized lifting and handling equipment.

7.27. Type B packages are designed to provide high impact and fire resistance and radiation shielding. These packages are designed to ensure that the material being transported should neither present a radiation hazard, nor release its contents, even if the package were involved in a severe accident. For this reason, Type B package designs should not only demonstrate the ability to withstand tests simulating normal shipping conditions but also withstand tests simulating severe accident conditions, without release of their contents and without significant increase in external radiation levels.

7.28. The construction of large Type B package designs (such as casks for the transport of irradiated fuel) required for meeting the safety objectives of containment of material and control of external radiation levels also provides some protection against malicious acts. Opening and accessing their contents is extremely difficult and requires the use of specialized tools and lifting equipment. Tests have shown that it is difficult, though not impossible, to sabotage or penetrate a Type B package.

Security overpacks and freight containers

7.29. A shipper may also use additional equipment beyond that required by the approved package design, such as overpacks. Overpacks are enclosures used by shippers to contain one or more packages of nuclear or other radioactive material to form a single handling unit. Shippers may use overpacks for several different purposes such as to consolidate several packages into a single handling unit for simpler and quicker loading or to enhance the security of the package by providing additional delay features. These systems can be open or closed, with special features to facilitate industrial handling equipment, incorporate unique locking mechanisms, or configured to be used on a specific type of conveyance.

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

7.31. Some of the safety control measures employed also serve as effective security measures. One example is the requirement for a fastening device for the containment system that cannot be unintentionally opened [13]. Another example is when package tie-down attachments required by the safety regulations can be secured (e.g. with locks) to provide delay and deter attempted removal of the package from the conveyance.

Package seals

7.32. Safety regulations require, in many instances and on many package designs, the use of package seals (e.g. tamper indicating devices) which are not readily breakable and which, while intact, will provide evidence that the package has not been opened or breached. Seals may also be present on packages of nuclear material to satisfy safeguards requirements. Seals may fulfil security functions such as inventory verification since many seals are uniquely identified with a specific alpha-numeric code. Paragraphs 5.7–5.15 provide detailed information on seals.

Maritime tracking

7.33. Maritime safety regulations, such as those derived from the IMO's International Convention for the Safety of Life At Sea (SOLAS) **Error! Reference source not found.** require communication systems that provide vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically **Error! Reference source not found.**.

7.34. The use of the automatic identification system for maritime transport presents an example of a transport safety and transport security challenge. The automatic identification system is used primarily to provide the user navigational information regarding vessels in their vicinity. This information supplements the information gained from the radar, distance of nearest point of approach of a vessel, time of nearest point of approach. The automatic identification system makes positive identification of the vessel for communications purposes. However, for security purposes and in some locations around the world, vessels might not wish to identify themselves. The safety and security implications should be carefully weighed when deciding to deactivate the automatic identification system, while consulting the relevant sections of the SOLAS regulations.

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, 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. 22), 2 vols, UNECE, New York and Geneva (2021).

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

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

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

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

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

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

[15] 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).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (D-Values), EPR D VALUES 2006, Emergency Preparedness and Response, IAEA, Vienna (2006).

[17] 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 (2022).

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

[19] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[20] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).

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

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

[23] 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).

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

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

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

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

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material (2018 Edition), IAEA Safety Standards Series No. SSG-26 (Rev. 1), IAEA, Vienna (in preparation).

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

[30] Mary Lynn Garcia, Design and Evaluation of Physical Protection Systems, (Second Edition), Butterworth-Heinemann (2008).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).

[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Security of Nuclear and Other Radioactive Material in Transport, IAEA-TDL-007, IAEA, Vienna (2018).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, NSS No. 8-G (Rev. 1), Vienna (2020).

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

[35] INTERNATIONAL MARITIME ORGANIZATION, International Convention for the Safety of Life At Sea, IMO (1974).

[36] INTERNATIONAL MARITIME ORGANIZATION, International Ship and Port Facility Security (ISPS) Code, IMO (2014).

[37] INTERNATIONAL MARITIME ORGANIZATION, International Maritime Dangerous Goods (IMDG) Code, IMO, London (2020).

[38] INTERNATIONAL MARITIME ORGANIZATION, International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships (INF) Code, IMO (2001).

[39] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Annex 17 to the Convention on International Civil Aviation Security, ICAO, Montréal, (2020).

[40] INTERNATIONAL AIR TRANSPORT ASSOCIATION, Security Management System Manual (SeMS), IATA (2021).