IAEA NUCLEAR SECURITY SERIES NO. XX

NST044

DRAFT, January 2016

STEP 8: Submission to MS for comment

Interface Document: NSGC, RASSC, TRANSSC

SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT

(REVISION OF NUCLEAR SECURITY SERIES NO. 9)

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

FOREWORD

(standard foreword to be inserted)

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Threats to nuclear security could include criminals acquiring and using radioactive material for malicious purposes to cause harm to individuals or the environment. Such threats could also include the dispersal of radioactive material through the sabotage of radioactive material packages during transport. The consequences of the malicious use of radioactive material could be high and radioactive material is potentially vulnerable during transport. This Implementing Guide is intended to assist States to reduce the likelihood of such events.

The IAEA addresses both the safety and security of radioactive material during transport. The Safety Standards Series include the Regulations for the Safe Transport of Radioactive Material (henceforth referred to as the Transport Regulations), the latest version of which was published in 2012 [1], the Fundamental Safety Principles, which were published in 2006 [2] and the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [3], are relevant to transport safety and include limited coverage of security[1].

Efforts were initiated in 2002 by the IAEA to provide guidance for security in the transport of radioactive material, based upon the new security requirements in the Recommendations on the Transport of Dangerous Goods — Model Regulations [4]. These provisions became part of the UN Model Regulations in late 2003 and have been updated regularly, the latest version being published in 2013. To provide a technical basis for establishing security levels for the protection of radioactive material in transport and appropriate security measures commensurate with the potential radiological consequences that could result from malicious use of radioactive material, the IAEA published an Implementing Guide on Security in the Transport of Radioactive Material as Nuclear Security Series No. 9 in 2008.

This Implementing Guide is a revision of the 2008 Guide, to better align this publication with the Nuclear Security Recommendations on Radioactive Material and Associated Facilities [5] published in 2011, to cross-reference other relevant Implementing Guides, and to add further detail on certain topics based on the experience of the IAEA and Member States in using the original Guide.

The UN Model Regulations provide the basis for security requirements for the transport of all dangerous goods and are implemented by States and international modal organizations. The security requirements for the transport of dangerous goods are found in Sections 1.4 and 7.2 of the Model

[1] (Nuclear) security means the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Regulations [4], incorporated in international transport in 2005. Other UN specialized agencies and programmes — e.g. the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO) and the United Nation Economic Commission for Europe (UNECE), and other intergovernmental organizations such as the Intergovernmental Organization for International Carriage by Rail (OTIF) and the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN) — have taken similar steps to provide improved security in the transport of all dangerous goods. IMO, ICAO UNECE, OTIF and ADN have also amended their respective international instruments [6–10] to reflect the security provisions of the UN Model Regulations.

1.2. OBJECTIVE

The objective of this publication is to provide guidance to States and their competent authorities on how to implement and maintain a nuclear security regime that provides for security in the transport of radioactive material to protect persons, property, society, and the environment from malicious acts, i.e. unauthorized removal, sabotage and attempts thereof, that could cause harmful radiological consequences. This publication may also be useful to shippers, carriers and others with transport security responsibilities. Since transport occurs in the public domain and frequently involves multimodal transfers, it is a potentially vulnerable phase of domestic and international commerce. This publication is intended to facilitate a uniform and consistent approach to security.

1.3. SCOPE

This guidance applies to the security of the international and domestic transport of packages containing radioactive material that may pose a radiological hazard to individuals, property, society and the environment as a consequence of a malicious act. It provides guidance for protection against unauthorized removal and sabotage. This protection is accomplished by a combination of measures to deter, detect (including assessment), delay and respond to such acts.

Some packages or types of radioactive material present such limited security concerns that they warrant only prudent management practices. Radioactive material with higher potential consequences needs to be protected at either a basic security level or an enhanced security level. This publication provides an activity threshold to identify packages that warrant the enhanced security level. In some situations (such as elevated threat) additional security measures may be appropriate and this publication provides some examples of such additional measures.

This publication also describes arrangements and measures to assist in the location and recovery of lost, missing or stolen radioactive material. More comprehensive guidance on this topic can be found in the Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of

Regulatory Control [11]. This publication does not address emergency preparedness and response aspects of a nuclear security event involving radioactive material in transport. These topics are covered in other IAEA publications [12-15].

Security and safety considerations for transport of radioactive material should work in concert to enable compliance with the Transport Regulations [1] as well as with other relevant IAEA safety standards and nuclear security guidance. Other regulations, standards, codes and guides developed for safety purposes may also apply, and can influence the design and implementation of a shipper's or carrier's transport security system. Care is also needed to ensure that safety measures do not compromise security and that security measures do not compromise safety.

The security measures for the transport of radioactive material defined in this publication are intended to protect against malicious acts, involving radioactive material and the resulting potentially harmful radiological consequences.

The Convention on the Physical Protection of Nuclear Material (CPPNM) [16], for which the IAEA is the depositary, provides a worldwide framework for ensuring the physical protection of nuclear material used for peaceful purposes while in international nuclear transport. It also applies, with certain exceptions, to nuclear material while in domestic use, storage and transport. The Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No.13 [17] recommends measures to protect against unauthorized removal and sabotage of nuclear material during transport. Ref. [17] discusses transport security with respect to the categorization of nuclear material, including specifics about thresholds for mass, enrichment and nuclides covered. The transport security measures proposed in this publication are complementary to the provisions in Ref. [17] and its supporting Implementing Guide, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G [18], on the security of nuclear material in transport. For some category III and below category III nuclear material there may be cases where the potential harmful radiological consequences of the material warrant additional security measures to those specified in Ref. [17] to protect against unauthorized removal. For example, because of their radioactivity, some category III and below category III nuclear material packages may warrant the enhanced security measures applying the methodology recommended in this publication. In respect of these particular cases, this publication provides measures additional to those contained in Ref. [17].

The security measures specified in this publication also give additional guidance on how the Code of Conduct on the Safety and Security of Radioactive Sources [19] and its supplementary document Guidance on the Import and Export of Radioactive Sources [20] could be implemented.

While the guidance presented in this publication is generally consistent with the UN Model Regulations [4] regarding to the number of security levels and the security measures recommended,

some specific security measures identified in Sections 4–6 are complementary to those in the Model Regulations.

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

1.4. STRUCTURE

This publication follows the structure of Ref. [5], as follows:

(a) Section 2 summarizes the objectives of the transport elements of a State's nuclear security regime for radioactive material and provides guidance on the principles, concepts and approaches for implementing the transport elements of a State's nuclear security regime for radioactive material.

(b) Section 3 describes how radioactive material is characterized for determining the appropriate transport security measures.

(c) Section 4 provides guidance on how a State may implement effective transport security elements within its nuclear security regime including specifying roles and responsibilities.

(d) Section 5 provides guidance on security measures to protect against unauthorized removal (including both mode independent measures and mode specific measures) and sabotage.

(e) Section 6 provides guidance on measures to locate and recover missing or stolen radioactive material.

(f) Appendix I provides background information on the establishment of activity threshold values for transport security measures, derived on the basis of the potential harmful radiological consequences of malicious acts involving radioactive material.

(g) Appendix II provides an example transport security plan and describes its content and structure.

(h) Appendix III provides information on transport security verification prior to transport.

To make this publication as complete, comprehensive and user-friendly as possible it contains both quotations from and references to Ref. [5]. Text quoted from Ref. [5] appears in italics and references in the text appear in parentheses (Ref. [5], para. x.y)

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

The overall objective of a State's nuclear security regime is to protect persons, property, society, and the environment from malicious acts involving nuclear material or other radioactive material that could cause unacceptable radiological consequences. The objectives of a nuclear security regime should include transport of radioactive material and should address:

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

The third objective is mainly related to radioactive material out of regulatory control, which is addressed in Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control.

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

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

Recognizing the societal benefits of using radioactive material, the nuclear security regime should strive to achieve a balance between managing radioactive material securely without unduly limiting the conduct of those beneficial activities." (Ref. [5], paras 2.1-2.4)

2.1. STATE RESPONSIBILITY

"The responsibility for establishment, implementation and maintenance of a nuclear security regime within a State rests entirely with that State." (Ref. [5], para. 3.1)

A State should take appropriate steps to provide a framework that will ensure a sound security regime exists within its State.

Each State has a responsibility to regulate radioactive material in transport in order to protect the material from malicious acts that could cause harmful radiological consequences to persons, property,

society, and the environment. Responsibility rests entirely with the State for ensuring that its security regime provides an effective framework for protection of radioactive material under its jurisdiction.

The State should ensure that its nuclear security regime includes elements for transport security of radioactive material. These security elements include: (a) the legislative and regulatory framework governing the security of the radioactive material in transport; (b) competent authorities, including a regulatory body, within the State responsible for ensuring the implementation of the legislative and regulatory framework; and (c) the transport-specific security systems and measures. Security systems in transport should be an integral part of the State's overall security regime for radioactive materials. The radioactive material transport security elements of the State's security regime should be reviewed and updated regularly by the competent authorities.

The State should ensure that its transport security regulatory body has effective independence. This means that organizational units responsible for licensing and supervisory activities have appropriate, sufficient and unfettered discretion in the execution of their tasks against any undue influence by other government agencies or external organizations in the execution of their tasks.

If the transport elements of the State's nuclear security regime are divided between two or more competent authorities, arrangements should be made for overall co-ordination. Clear lines of responsibility should be established and recorded between the relevant entities so that continuous protection of the material is ensured.

"The State should ensure that the regulatory body and other competent authorities are adequately provided with the necessary authority, competence and financial and human resources to fulfil their assigned nuclear security responsibilities." (Ref. [5], para. 3.7)

States should clearly assign security responsibilities to the shipper, carrier, receiver or others engaged in the transport of radioactive material. For example, States may choose to hold the shipper solely responsible for security during transport, requiring that the shipper either conduct the transport operation themselves or use a carrier which implements security measures under the direction of the shipper. Alternatively, the State may choose to assign the responsibilities for security to authorized carriers and allow the shipper to rely on the carrier's security system. In any case, these responsibilities should be clearly allocated. General responsibilities that the State may assign include developing a transport security plan, providing advance notification of the shipment details to the receiver and completing other relevant technical, procedural and administrative activities.

States should establish appropriate mechanisms to cooperate, consult and exchange information on security techniques and practices for transport, within the constraints of confidentiality. States should assist each other in recovering stolen or missing radioactive material when requested. Appropriate arrangements may be established between shipping, receiving and transit States, and relevant

intergovernmental organizations, to promote cooperation, harmonization and information exchange, and to ensure that radioactive material under their jurisdiction is adequately protected.

The State should establish State-level security contingency plans to respond to unauthorized removal of radioactive material or sabotage of packages containing such material, or attempts thereof. These plans should describe measures that the State is prepared to undertake in the event of theft or sabotage involving radioactive materials during transport. The plans should cover both domestic and international transports of radioactive material. They should be coordinated with the State emergency plans for response to a nuclear or radiological emergency in line with the all hazards approach [14-15].

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

2.2. INTERNATIONAL TRANSPORT

A State's nuclear security regime should ensure adequate protection of radioactive material not only within its own borders but also when on ships and aircraft registered to that State while in international waters or airspace and until responsibility is transferred to another State.

Coordination between importing and exporting States should be established prior to transport, to reduce the likelihood of malicious acts in connection with the import or export of quantities of radioactive material above defined thresholds. As a minimum, these steps should encompass requirements consistent with the Guidance on the Import and Export of Radioactive Sources [20] for Category 1 and 2 radioactive sources.

International shipments may involve land transport by road or rail, intermodal transfers, transport by aircraft or ships, transit through multiple States and in-transit storage. The relevant competent authority should require the shipper/carrier to maintain the security of the radioactive material throughout transport and that any transfer of responsibilities for the security of the material is clearly defined.

2.3. LEGISLATIVE AND REGULATORY FRAMEWORK

2.3.1. State

The State should establish, implement, and maintain an effective national legislative and regulatory framework to regulate the security of radioactive material in transport, which:

(a) Includes goals and objectives in the development of transport security regulations;

(b) Takes into account the risk of malicious acts involving radioactive material that could cause unacceptable radiological consequences;

(c) Prescribes and assigns governmental responsibilities to competent authorities, including an independent regulatory body separate from carriers and shippers;

(d) Assesses its domestic threat and applies that threat information in establishing regulatory requirements;

(e) Defines the radioactive material which is subject to the nuclear security regime in terms of nuclides and quantities of radioactive material present;

(f) Places the prime responsibility on the shipper and/or carrier for implementing and maintaining security measures for radioactive material during transport;

(g) Establishes an authorization process for security of radioactive material in transport, which may include issuance of specific licences or other forms of authorization according to a graded approach;

(h) Integrates, as appropriate, the authorization process for transport security of radioactive material with that for safety or radiation protection;

(i) Establishes a procedure for submission of a transport security plan by the shipper and/or carrier and, as appropriate, for approval of the plan by the competent authority prior to transport;

(j) Prescribes requirements for the design and evaluation of the transport security system, by the shipper/carrier as appropriate;

(k) Reviews the security requirements on a regular basis to take account of advances in technology and potential changes in the threat;

(l) Establishes an inspection process for security requirements;

(m) Establishes a programme for verifying continued compliance with security requirements in particular through periodic inspections and desktop reviews, and ensuring that corrective actions are taken when needed;

(n) Establishes enforcement mechanisms and processes for the failure to comply with security requirements;

(o) Establishes penalties that may be applied for non-compliance with the requirements;

(p) Takes into account the interface between security and safety of radioactive material.

(q) Establishes a policy to identify, classify and control sensitive information, the unauthorized disclosure of which could compromise the security of radioactive material in transport;

(r) Includes requirements, consistent with national practices, for ensuring the trustworthiness of persons with authorized access to sensitive information or to radioactive material during transport or who have specific security responsibilities during transport;

(s) Establishes security clearance procedures, for persons engaged in the transport of radioactive material, commensurate with their responsibilities, e.g. requirements for positive identification of such persons;

(t) Establishes requirements for reporting of security related events, including missing or lost packages of radioactive material; and

(u) Establishes sanctions that may be applied against the unauthorized removal of radioactive material and sabotage during transport.

2.3.2. Regulatory body

The regulatory body responsible for transport security should implement the legislative and regulatory framework and, as appropriate, authorize transport activities only when they comply with its security regulations. Where it is required, the review of the applicant's Transport Security Plan can be used by the regulatory body in determining whether to issue an authorization.

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

The regulatory body should verify continued compliance with its transport security regulations and, as appropriate, relevant authorization conditions notably through inspections and desk top reviews and ensuring that corrective action is taken, when needed. Inspections of security measures implemented by shippers, carriers and receivers could be coordinated with inspections by other regulatory bodies responsible for verifying compliance with other regulatory requirements, such as radiation protection and safety. However as far as sensitive information is concerned this may not be possible for information security reasons. The functions of the regulatory body should include:

(a) Defining requirements for security during transport based on the threat assessment or if applicable the design basis threat (DBT) [21] or an alternative threat statement (see section 2.4) in order to protect against both unauthorized removal and sabotage;

(b) Specifying requirements for Transport Security Plans (TSP);

(c) Licensing or otherwise authorizing shippers and/or carriers to transport radioactive material when such a licence or authorization is required;

(d) Performing inspections (both announced and unannounced) and desktop reviews, when needed, of radioactive material transports to ensure shipments are undertaken in compliance with the applicable requirements and conditions established by the regulatory body;

(e) Performing evaluations of the transport security systems, consistent with a graded approach and including exercises where appropriate, depending on the regulatory approach chosen by the State;

(f) Ensuring trustworthiness determinations are made, using a graded approach, for all personnel that have security responsibilities during transport or access to sensitive information;

(g) Defining what transport related information should be considered as sensitive and ensuring that its confidentiality is protected accordingly if appropriate;

(h) Enforcing applicable requirements and ensuring corrective actions are taken when needed; and

(i) Effective liaison with other competent authorities concerned, in particular those responsible for transport safety and agencies responsible for import and export control

2.3.3. Shipper, carrier and receiver

The legislative and regulatory framework should require that the shipper, carrier and receiver:

(a) Comply with and implement all applicable regulations and requirements;

(b) Ensure that all security measures and arrangements are in place and operational and that all the necessary permits and authorizations have been obtained prior to the commencement of transport;

(c) Establish quality management systems that provide:

— Assurance that applicable transport security requirements are satisfied;

— Control mechanisms and procedures for reviewing and assessing the overall effectiveness of security measures;

(d) Report to the regulatory body and/or to any other designated competent authority, all security events involving radioactive material transport; or

(e) As necessary, cooperate with and assist any relevant competent authorities in case of a security event involving radioactive material transport.

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

When authorized by the State the receiver may be assigned some of the responsibilities of the shipper/carrier. For example, for import shipments the receiver may have the primary responsibility for implementing security of radioactive materials once the shipment arrives in the importing State.

The carrier should be held responsible for ensuring that the functions it performs are in compliance with applicable national regulations. These may include:

(a) Providing a conveyance and crew that complies with all applicable safety and security requirements including crew fitness for duty (trustworthiness, drug testing, training, licensing), conveyance suitability and maintenance requirements;

(b) Ensuring that any carrier-provided equipment is suitable for the application and satisfies regulatory requirements; and

(c) Ensuring that in the event of an incident during transport, carrier personnel are prepared to act in accordance with the emergency and contingency plans.

2.3.4. Subcontracting

The regulatory body should require that, if subcontractors are used during the shipment, the contracting party ensure that the subcontractor is fully aware of applicable security requirements and be satisfied that the security arrangements are maintained throughout the shipment. In case a licence or authorization is required to perform transport activities, the contracting party should ensure that its subcontractor is duly licensed or authorized.

2.3.5 Deficiencies

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

The regulatory body should require that, if any deficiencies are discovered by the crew during transport, they be reported immediately to their management and compensatory measures taken.

2.4. ASSESSMENT OF TRANSPORT SECURITY THREATS

The State should assess and periodically review its national threat for radioactive material during transport and should evaluate the implications of any changes in the threat level.

The regulatory body should base its transport security requirements on this evaluation of the threat and require security measures appropriate to counter the threat. Additionally, the regulatory body may choose to communicate threat information, including changes in the threat, to the shipper/carrier to aid in the development of its security system and TSP. Such information should be appropriately protected due to its sensitive nature.

States will vary in their ability to identify and evaluate threat information. Some States have sophisticated security and intelligence capabilities that can assist the competent authorities in understanding the nature and extent of threats, including those that might be directed toward radioactive material transport. In other cases, general information about the national threat such as civil unrest, criminal activities and terrorist presence should be evaluated to identify the potential

threat. In all cases this should be done cooperatively among the State agencies that have responsibilities for understanding and responding to threats (intelligence, police, military etc.).

The State may wish to develop a design basis threat or alternative threat statement (ATS) in order to communicate threat information to relevant organizations. Development of a DBT and an ATS entail similar steps, but the ATS approach is less rigorous and formal and generally involves fewer organizations. If the State does not have sufficient resources to conduct the formal process of DBT development, or if the DBT process does not bring sufficient benefit in terms of reducing the risk associated with the radioactive materials to be protected, then an ATS can be defined. A description of the motivations, intentions, and capabilities of potential adversaries that is less rigorous and formal than the approach used to establish a design basis threat.

It is also possible that a State defines a DBT for radioactive material with higher potential radiological consequences, and an ATS for lower potential consequence material.

The regulatory body should provide guidance to the shipper, carrier, receiver and others engaged in transport of radioactive material on recognizing the potential for insider threats within their organization. Security systems should be designed, in a graded manner, to protect against the insider threat, particularly for personnel that exercise control over a shipment (such as a truck driver). Additional information on DBT and ATS can be found in Ref. [21].

2.5. RISK BASED TRANSPORT SECURITY SYSTEMS AND MEASURES

2.5.1. Risk management

The State should use a risk management approach to ensure that its nuclear security regime is keeping the risk of unauthorized removal or sabotage during transport at an acceptable level. This approach includes evaluating the threat and potential consequences of such acts and ensuring that appropriate security measures are put into place to protect against malicious acts.

Risk management takes into account an assessment of risk which can be quantitative or qualitative. Quantitative risk assessment involves determining the likelihood of an event occurring and multiplying it by the potential consequences of the event. The likelihood of a malicious act occurring or being attempted is very difficult to quantify and therefore in some cases is assumed to be one. Qualitative risk assessment involves consideration of the threat and potential consequences in order to identify combinations (e.g. high threat and severe consequences) where efforts should be focused to minimize risk. Similarly, low risk combinations illustrate where the graded approach should be also applied and security measures do not need to be as stringent.

A risk matrix is a matrix that can be used to illustrate the various levels of risk as a function of the likelihood and consequences of a security event. This is a simple mechanism to increase visibility of risks and assist the State decision making process. Figure 1 is an example of a risk matrix.

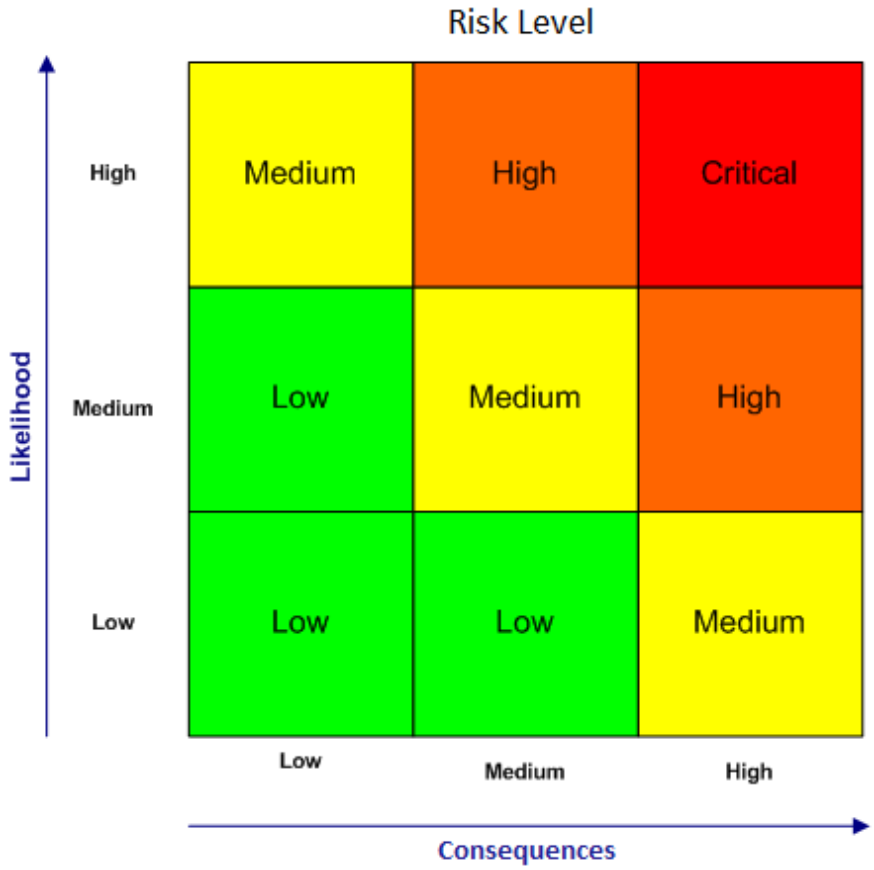

FIG. 1. Risk matrix.

The results of the risk assessment identify areas where vulnerabilities should be further evaluated to determine if strengthened measures should be required to reduce the security risk. Risk can be reduced through, for example, deterrence (appearance of robust security measures), strengthening security measures (e.g. additional defence in depth, increasing the conveyance/package resistance to attack, strengthened information security) and reducing potential consequences (e.g. the chemical or physical form of the material being transported).

The State should decide what level of risk is acceptable and what level of effort is justified to protect radioactive material in transport against the threat so as to reduce the risk to an acceptable level, given the availability of resources, the benefit of the protected asset to society, and other priorities. The required security measures may take advantage of other measures established for radiological safety purposes.

The regulatory body should develop requirements by using a graded approach applying the principles of risk management including the categorization of radioactive material according to its risk level.

2.5.2. Graded approach

Security requirements for radioactive material should be based on a graded approach, taking into account the principles of risk management, including such considerations as the level of threat and the relative attractiveness of the material.

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

In addition to using the concept of the graded approach for specifying requirements for physical protection, a State should consider the use of this concept to define the levels for other security measures, such as those addressing information protection and trustworthiness of individuals.

2.5.3. Defence in depth

Transport security requirements should incorporate the principle of defence in depth which is the concept of including several layers and methods of protection that have to be overcome or circumvented by an adversary in order to complete a malicious act. Such requirements should include a designed mixture of hardware (security devices), administrative measures (including the organization of personnel and the performance of their duties) and the design of the transport equipment (conveyance, any protective over-packs and package).

The regulatory body should require that the defence in depth approach is incorporated in the design of the transport security system for the functions of detection, delay and response. Based on a graded approach, each function may have independent capabilities so that failure of one capability does not mean loss of that function. For example, detection can rely on observation by personnel and also use electronic measures to detect intrusion into the cargo compartment. Applying a graded approach, delay can consist of multiple independent physical barriers such as the conveyance enclosure, over-packs with protective features, the package and securing these so the adversary task time is increased.

2.5.4. Methods for specifying risk-based security provisions

The basic steps for specifying risk-based transport security measures are:

(a) Performing a threat assessment within the State, based on information from security and intelligence experts;
(b) Evaluating the potential consequences of malicious acts involving radioactive material;
(c) Establishing the security levels to be applied to radioactive material packages or conveyances;
(d) Defining security objectives for each security level;

(e) Specifying administrative and technical requirements or specific security measures necessary to meet the security objectives.

When specifying security measures the regulatory body will need to make a number of decisions regarding the stringency of those requirements based on threat, risk and the feasibility/cost of implementation. Such decisions may result in specifying more stringent security measures for shipments of Category 1 radioactive sources as compared to Category 2 radioactive sources, such as requiring:

(a) Electronic position monitoring of conveyances
(b) Additional crew members
(c) Guards and/or law enforcement personnel
(d) Escort vehicles

2.5.5. Safety and security interface

Recognizing that both safety and security need to be addressed when making a shipment, a well-coordinated approach between these areas is necessary.

For the transport of radioactive material the State should ensure that:

(a) A balance is maintained between safety and security throughout the nuclear security regime, from the development of the legislative framework to implementation of safety and security measures;
(b) Regulatory requirements are consistent, especially when responsibility for safety and security is assigned to different competent authorities;
(c) Safety requirements do not compromise security and that security requirements do not compromise safety;
(d) Coordination between authorities in charge of nuclear safety and of nuclear security is ensured;
(e) Safety and security interfaces are strengthened by promoting both safety and security cultures into the integrated management system;
(f) During normal and emergency situations security measures for radioactive material in transport take into account those measures required for safety and vice versa;
(g) To the extent possible security measures during a response to a nuclear security event do not adversely affect the safety of the transport personnel and the public.

Some measures required by the safety regulations are also beneficial to providing security. For example, the seal required on all Type A, B, C and fissile packagings fulfil the security function of providing evidence that the package has not been opened. The tie-downs required to secure a package to the conveyance may also be suitable for affixing security equipment such as locks. However, not

all tie-downs are suitable for security purposes, such as those constructed of webbing or other materials that are not resistant to cutting.

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

Consideration should also be taken where there is a possible conflict of safety and security measures during transport such as placarding and labelling, route and mode selection; and information management (openness for safety and confidentiality for security). For example, when escorting personnel can provide emergency response and are aware of the nature and hazards of the material, external hazard communication may not be necessary on an exceptional basis. Solutions to potential conflicts such as these should be assessed and approved by the regulatory bodies responsible for transport safety and security

2.6. SUSTAINING TRANSPORT SECURITY

Sustaining the State's nuclear security regime is necessary to ensure it remains effective in the long term.

2.6.1. Security culture

"Security Culture: All organizations involved in implementing physical protection should give due priority to the security culture; to its development and maintenance necessary to ensure its effective implementation in the entire organization." (Ref. [22], para. 1.1)

Nuclear security culture plays an important role in ensuring that individuals, organizations and institutions remain vigilant and that security measures are sustained to protect against sabotage or unauthorized removal of radioactive material during transport. An effective security culture is dependent on proper planning, education, training, awareness, operation and maintenance, as well as on people who plan, operate and maintain the security systems. Even a well-designed system can be degraded if one or several components necessary to operate and maintain it are poor or fail, such as in the case where the shipper/carrier fails to follow procedures.

All personnel involved in transport operations should be aware of the need to establish and maintain an effective security culture. Such awareness can be achieved by regular briefings on strong and effective security practices and strong procedural adherence. For further information, see Ref. [22].

2.6.2. Quality management system

The regulatory body should require that shippers, carriers and receivers establish, implement and maintain quality management systems to ensure that security systems are designed, implemented, operated and maintained to perform as required. In particular, the quality management system should ensure that all relevant security measures, such as tracking system and communications equipment, are operating correctly. The quality management system should encompass all security related activities (technical, procedural and administrative) and should be reviewed on a periodic basis. The quality management system should include:

(a) Operating procedures and instructions to personnel (specific to role);
(b) Human resources management and training;
(c) Equipment – maintaining, updating, repair and calibration;
(d) Performance testing and monitoring of operating systems;
(e) Configuration management – ensuring the physical protection system (including computer systems) is configured as designed and that any changes are properly designed, verified and implemented; and
(f) Resource allocation to ensure continued performance of the security system.

Quality management systems for safety applications are influenced by the need for openness and transparency. While the quality management systems for security will be based on similar approaches, consideration should be given to the need for protection of sensitive information in addition to other assets. The management system should comply with international standard such as ISO 9001. Certification by an accredited agency may be acceptable for meeting the quality management system requirements.

2.6.3. Information security

Access to security-sensitive information should be limited to those people who need that information in order to perform their jobs. Key elements of information security include identifying the information that needs to be protected, designating individuals with authorized access to such information, and protecting such information from disclosure to individuals who do not have this access.

In particular, sensitive parts of the transport security plan should be subject to information security measures.

The regulatory body and other competent authorities should take steps, consistent with national requirements and procedures, to ensure appropriate protection of specific or detailed information relating to transport operations and security systems, the unauthorized disclosure of which could

compromise security. These steps include identifying what information needs to be protected and the level at which it needs to be protected, using a graded approach. The regulatory body should require that shippers, carriers and receivers follow specific provisions for information security.

Because certain information may need to be shared with a range of recipients for operational purposes (ferry bookings and transport network requirements), protection of such information should be adequate yet not so stringent that it adversely affects transport operations.

The State should establish sanctions that may be applied for violation of information security requirements. They should be sufficiently severe to act as a deterrent against such actions, commensurate with the sensitivity of the information disclosed.

2.6.4. Sustainability programme

The State should establish a sustainability program to ensure that the necessary resources are committed to the continued effectiveness of its nuclear security regime. This should include ensuring that the regulatory body and other competent authorities are provided with adequate resources for fulfilling their responsibilities.

For detailed guidance, see Ref. [23].

2.7. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

The State should ensure that competent authorities, shippers, carriers and all others involved in the transport of radioactive are trained and prepared to respond if a malicious act occurs against a shipment of radioactive material. This should be achieved by contingency planning, which may include periodic rehearsals, tests or exercises.

The regulatory body should establish requirements for shippers, carriers, receivers and others engaged in transport security to have appropriate and effective security measures to detect nuclear security events and to promptly report and respond to such events.

The State’s regulatory framework should clearly specify the requirements, the roles and responsibilities for emergency planning; what emergency response capabilities are to be provided by the State, what are to be provided by the operators and relevant stakeholders, and how these are to be coordinated [14-15].

Arrangements should be made to ensure the continued effectiveness of the security system during any emergency.

3. CHARACTERIZATION OF RADIOACTIVE MATERIAL FOR TRANSPORT SECURITY

Radioactive material should be characterized to determine appropriate security requirements to prevent unauthorized removal or sabotage during transport. This takes into account the potential radiological consequences of unauthorized removal or sabotage and subsequent dispersal (e.g., in a radiological dispersal device (RDD)) or use for other malicious purposes. When multiple radionuclides are transported together (e.g., in the same package or conveyance) the aggregation of material also needs to be considered.

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

3.1. RADIOACTIVE MATERIAL CATEGORIZATION

A categorization system should be established to implement the graded approach. Security levels (required degrees of protection) should be associated with specific types and quantities of radioactive material defined by the categorization system, thereby identifying when greater levels of protection are warranted for radioactive material that could result in higher consequences if used in a malicious act.

The material to be transported should be characterized to identify the radionuclides, the form and activities involved. In some cases a shipment may consist of a single radionuclide, either in a single package or multiple packages. In other cases, there may be multiple radionuclides within a single package or multiple packages containing multiple radionuclides. In all cases, the identity and activity level of the radionuclides should be determined.

A State should determine an appropriate basis for categorization of radioactive materials for domestic and international transport. Categorization may be done on a ‘per conveyance’, ‘per consignment’ or ‘per package’ basis. When organizing an international transport, an operator should always take into account the domestic approaches chosen by the States involved. These options are summarized as follows:

(a) The ‘per package’ basis is the simplest approach to apply, but does not account for multiple packages being transported together;

(b) The ‘per consignment’ basis makes it easy to determine category by adding the activity of all packages offered by a shipper at one time, but does not account for multiple consignments from multiple shippers on a single conveyance; and

(c) The ‘per conveyance’ basis provides the best measure of security significance since all the packages on a conveyance could be seized in a single adversarial action. However, it is very difficult to apply to international air and sea transport where consignments may be consolidated; may lead to frustration of shipments due to carriers not wanting to deal with the complexity of keeping track of activity on-board a conveyance;

The international dangerous goods transport regulations use two categories of material for application of security requirements – all dangerous goods; and, high consequence dangerous goods. Since radioactive materials are one class of dangerous goods, consistency with the dangerous goods regulations is desirable in order to facilitate their transport without unnecessary complications. Therefore, two categories of radioactive material should be used for the application of security measures. These two categories can be established using an activity threshold to separate them by security significance.

Depending on the radionuclide, this threshold should be based on the ‘D value’ or the ‘A value’ for the particular radionuclide.

The D value is the radionuclide-specific activity of a sealed radioactive source which, if not under control, could cause severe deterministic effects for a range of scenarios that include both external exposure from the unshielded source and internal exposure following dispersal of the source material. The D values can be found in Annex I of the IAEA Code of Conduct on the Safety and Security of Radioactive Sources [19]. For radionuclides listed therein the D value should be used in establishing the threshold.

All commonly transported radionuclides are assigned A values in the IAEA Regulations for the Safe Transport of Radioactive Material, SSR-6 [1]. These values represent the maximum activity that can be safely transported in a Type A or non-accident resistant package. There are two A values listed in SSR-6, A_1 and A_2, for different forms of material. For security purposes, the A_2 value should be used. For radionuclides not listed in the Code of Conduct for the Safety and Security of Radioactive Sources [19], the A_2 value should be used in establishing the threshold.

Evaluations were made of the potential radiological consequences for a variety of radionuclides in a dispersion scenario (see Appendix I). The results of these evaluations led to a recommended activity threshold of:

(a) For radionuclides listed in the IAEA Code of Conduct for the Safety and Security of Radioactive Sources [19], an activity equal to or exceeding that for a Category 2 radioactive source (also known as 10 D or ten times the D value); and,

(b) For all other radionuclides, an activity of 3000 A_2 or greater.

The application of this threshold results in two categories of radioactive material – those with activities below the threshold and those with activities above the threshold.

A State should define radioactive material that poses very low potential radiological consequences and does not represent a substantial security concern. Packages containing these materials do not need to be assigned a security level and only need to be controlled through prudent management practices.

For radioactive material transported in excepted packages and for LSA-I and SCO-I (see SSR-6 for further information), no specific security measures beyond the control measures required by the safety regulations and prudent management practices already implemented by shippers and carriers are recommended.

Such material includes:

(a) UN 2908 EXCEPTED PACKAGE – EMPTY PACKAGING;
(b) UN 2909 EXCEPTED PACKAGE – ARTICLES MANUFACTURED FROM NATURAL URANIUM or DEPLETED URANIUM or NATURAL THORIUM;
(c) UN 2910 EXCEPTED PACKAGE – LIMITED QUANTITY OF MATERIAL (containing 10^{-3} A_2 or less per package);
(d) UN 2911 EXCEPTED PACKAGE – INSTRUMENTS OR ARTICLES (containing A_2 or less per package);
(e) UN 2912 RADIOACTIVE MATERIAL, LOW SPECIFIC ACTIVITY (LSA-I);
(f) UN 2913 SURFACE CONTAMINATED OBJECTS (SCO-I),
(g) UN 3507, URANIUM HEXAFLUORIDE, RADIOACTIVE MATERIAL, EXCEPTED PACKAGE, less than 0.1 kg per package, non-fissile or fissile excepted.

3.2. ASSIGNING SECURITY LEVELS

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

Packages containing activity values less than the threshold value should be assigned to the "basic" security level.

Packages containing activity levels equal to or greater than the threshold value should be assigned to the "enhanced" security level.

Some packages assigned to the enhanced security level can contain very high activity contents. For example, some packages containing radioactive sources may have contents up to several hundred thousand times the D values. Because of this wide range of activity in the enhanced security level (ranging from 10 D to several hundred thousand D), States may wish to establish subcategories within the enhanced security level and specify security measures for each subcategory. For example,

packages containing between 10 and 1000 D (Category 2) may be required to have a specified set of security measures and packages containing more than 1000 D (Category 1) may be required to have a more stringent set of measures.

3.3. RADIOACTIVE MATERIAL AGGREGATION

In some cases it is necessary to aggregate radioactive material in order to determine whether or not a package or collection of packages exceeds the transport security activity threshold for the enhanced security level, such as:

(a) When more than one radionuclide are transported in the same package (for example, a moisture density gage containing Cs-137 and Am-241/Be); or

(b) When the State requires aggregation of packages for domestic transport.

Determination of whether or not the transport security activity threshold has been met or exceeded in such cases can be calculated by summing the ratios of activity present for each radionuclide divided by the transport security threshold for that radionuclide. If this sum is less than 1, then the activity threshold has not been exceeded.

This calculation can be made with the formula:

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

Where:

A_i = activity of radionuclide *i* that is present (TBq)

T_i = transport security threshold for radionuclide *i* (TBq).

3.4. POTENTIAL RADIOLOGICAL CONSEQUENCES OF SABOTAGE

Sections 3.1–3.3 above address categorizing and assigning radioactive material to security levels based on the potential consequences of unauthorized removal and subsequent dispersal. Security systems designed to protect radioactive material from unauthorized removal generally also provide some degree of protection of the radioactive material against sabotage. However, in some cases specific security measures to protect against sabotage may be warranted based on their potential to cause unacceptable radiological consequences.

The State should determine which shipments warrant protection against sabotage because of their potential to cause unacceptable radiological consequences. States may have varying judgments on what constitutes unacceptable radiological consequences. For additional guidance on determining what constitutes unacceptable radiological consequences see the implementing guide Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Rev. 5) [24].

Based on that determination, States should identify which shipments may require protection against sabotage. Factors that should be considered include:

(a) Package contents (radionuclides, activities, physical and chemical forms)
(b) Package and conveyance design;
(c) Effect of the postulated sabotage event (or events) on the contents/package/conveyance combination; and
(d) Location where the act of sabotage may occur (e.g., in a highly populated area if transport of such material is allowed in these areas).

Section 7 provides additional detail on how potential radiological consequences from acts of sabotage can be determined and security measures that the State might wish to require.

3.5. ATTRACTIVENESS OF RADIOACTIVE MATERIAL IN TRANSPORT

The attractiveness of radioactive material to potential adversaries should be considered. This can be done by considering:

(a) Chemical and physical form (solubility, powder, etc.)
(b) Radiation emission type (alpha, beta, gamma)
(c) Solubility, respirability, and
(d) Half-life of the radionuclides.

These factors influence the ease of dispersion of the material and the potential radiological consequences of a malicious act.

For shipments of material that the State determines are particularly attractive, it may wish to adjust the security level (e.g., increase the security level from basic to enhanced) or specify more stringent security measures.

4. ESTABLISHING A REGULATORY PROGRAMME FOR TRANSPORT SECURITY

This section provides guidance to regulatory bodies on how to develop or enhance regulatory programs to address the security of radioactive material during transport.

4.1. SPECIFYING AND APPLYING TRANSPORT SECURITY REQUIREMENTS

"The regulatory body should establish goals or objectives that define the required outcome of nuclear security systems for each security level." (Ref. [5], para. 4.6)

The regulatory body should select a regulatory approach that the shipper, carrier, receiver and others engaged in transport is required to follow to meet goals and objectives of the required outcome. There are three alternative approaches that the regulatory body may use:

(a) A prescriptive approach, in which the regulatory body directly specifies the security measures that the shipper, carrier, receiver and others engaged in transport should implement to meet the goals and objectives, or

(b) A performance-based approach, in which the regulatory body requires the shipper, carrier, receiver and others engaged in transport to design the nuclear security system and demonstrate to the regulatory body that the nuclear security systems meets the goals and objectives, or

(c) A combined approach, in which the regulatory body draws on elements of both the prescriptive and performance-based approaches.

Under all three approaches, the nuclear security system needs to achieve the required outcome defined by the goals and objectives for the applicable security level. This is the standard by which all nuclear security systems are evaluated.

4.1.1. The prescriptive approach

Regulatory requirements based on the prescriptive approach require the shipper, carrier and receiver to implement specific security measures to meet the security objectives for the applicable security level. A set of recommended security measures is provided in Section 5.

Advantages of the prescriptive approach include: simplicity in implementation for the regulatory body and the shipper, carrier, receiver and others engaged in the transport of radioactive material; elimination of the need to transmit sensitive threat information; and ease of inspection and auditing.

The disadvantage of the prescriptive approach is its relative lack of flexibility in addressing actual circumstances. The use of the prescriptive approach may be particularly appropriate in cases where the combination of threat and potential consequences is low.

4.1.2. The performance-based approach

Performance based regulatory requirements require the shipper and/or carrier to design and implement a security system that meets applicable security objectives against the threat, but allows flexibility in choosing the particular security measures to be implemented. In designing the security system to meet the objectives, the shipper and/or carrier needs to counter the threat as defined by the State.

The performance based approach allows flexibility for the shipper, carrier, receiver and others engaged in the transport of radioactive material to propose a particular combination of security measures. The adequacy of these measures is then assessed against the threat.

The advantage of this approach is that it recognizes that an effective transport security system can be composed of many combinations of security measures tailored to individual circumstances that are

capable of meeting the security objectives. The performance based approach is also the most cost effective approach when the necessary knowledge and skills are available.

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

4.1.3. The combined approach

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

(a) The regulatory body may require application of a performance-based approach for the radioactive materials having the highest potential consequences of malicious use, while allowing application of a prescriptive approach for lower consequence materials.

(b) The regulatory body may require that a set of prescriptive requirements be supplemented by using the performance based approach to address particular matters such as an increase in threat.

(c) The regulatory body may adopt a set of alternative security measures from which the security system designer may choose. The security system designer should then demonstrate that its resulting transport security system, as a whole, meets the applicable security objectives.

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

4.1.4 Process for applying the approach

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

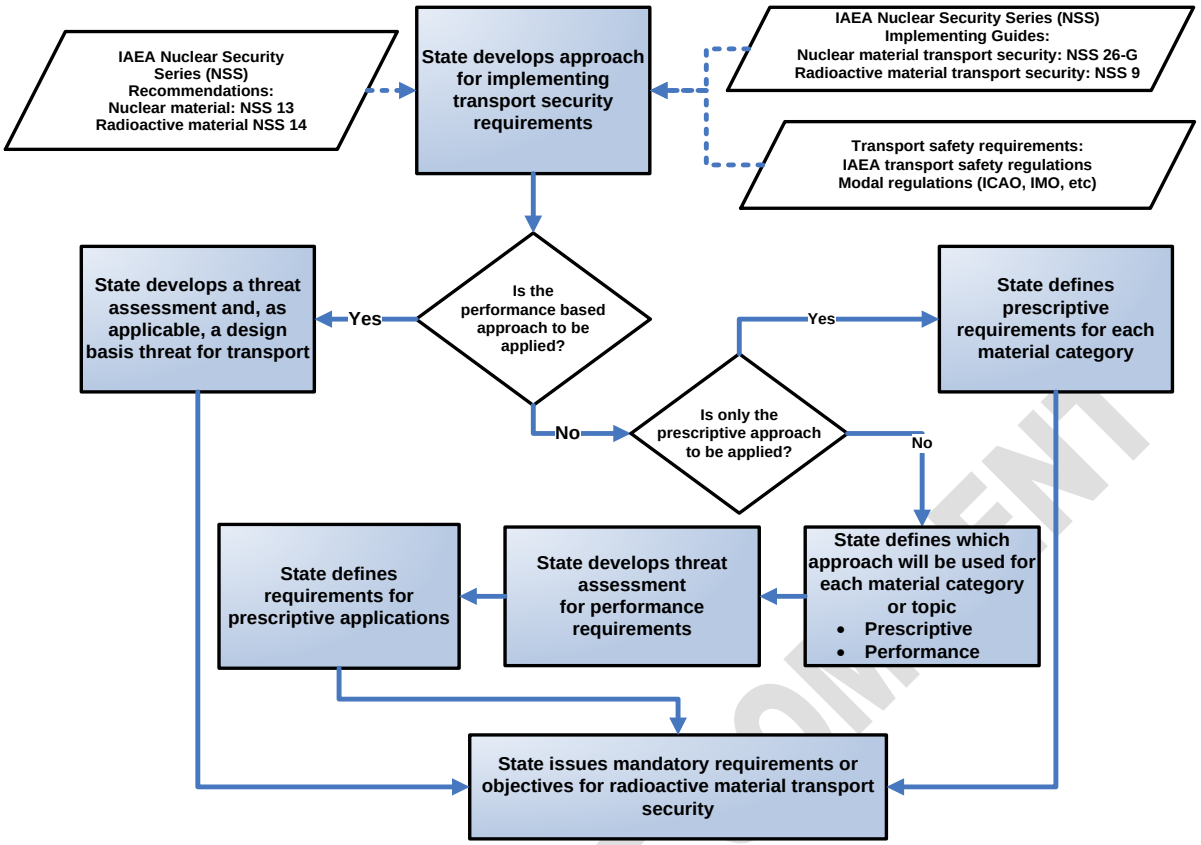

FIG. 2. Decision process for determining the regulatory approach to transport security ICAO: International Civil Aviation Organization; IMO: International Maritime Organization.

4.2. FUNCTIONS OF A TRANSPORT SECURITY SYSTEM

The transport security system should be designed to adequately perform the security functions of detection, delay, and response in order to deter and prevent an adversary from completing a malicious act. The security system should also include security management measures which provide, inter alia, for the integration of people, procedures, and equipment through the application of administrative measures.

"The transport security system should be designed to take into account the:

- *Quantity and the physical and chemical form of the radioactive material;*
- *Mode(s) of transport;*
- *Package(s) being used."* (Ref. [5], para. 4.30)

When visible, security measures defined for each security function may provide deterrence. These measures could include visible security measures built into the conveyance such as the use of guards, robust package and padlocks.

The fundamental concepts of detection, delay, and response apply to all categories of radioactive material; however, their implementation should be accomplished in a graded manner and considered in the context of the States threat assessment.

4.2.1 Detection

Activities directed toward the detection of unauthorized removal, sabotage and other intentional malicious acts should start before the radioactive material is placed on or in the load carrying conveyance and continue until the shipment has been completed. For example, inspections of vehicles before loading packages on board can help ensure that the vehicle has not been tampered with and nothing has been affixed to the vehicle that might compromise security.

Continuous surveillance is frequently used for the function of detection. The conveyance crew and/or the guards involved in the shipment can provide continuous surveillance of the transport conveyance and the surrounding area.

Detection can also be achieved through the use of technical measures such as electronic sensors, video surveillance, audio surveillance, tracking devices, shipment monitoring and duress notification devices, e.g. for drivers and escort personnel.

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

In implementing a graded approach, the objectives of detection measures could range from immediate detection, assessment and communication of any unauthorized access (during an attempted malicious act) to detection of unauthorized removal through tamper indicators or verification during reloading (after the material has been removed).

4.2.2 Delay

Delay measures in transport should increase the time required to remove the material from the conveyance in order to enable an appropriate and effective response. A measure of delay is the time, after detection, that is required by an adversary to complete a malicious act.

Delay measures should be implemented through physical means, such as locked doors, over-packs, cages and locking tie-downs, as well as measures such as properly equipped and trained guards.

In implementing a graded approach that takes into account the category of the radioactive material, the objectives of delay measures could range from providing sufficient delay after detection to allow response personnel to interrupt any malicious acts to providing delay to assist in timely pursuit following unauthorized removal.

4.2.3 Response

Response measures should be implemented following detection and verification that a security event is underway. The shipper, carrier, receiver and others engaged in the transport should be required to

make appropriate arrangements to communicate with law enforcement personnel following the confirmation of a security event in order that they may undertake the response.

The response to a security event may be provided by crew members, accompanying guards or local or regional authorities. Response activities should have the objective of interrupting a malicious act with sufficient resources to prevent completion of the act.

4.2.4 Security management

Security management includes the establishment and implementation of policies, plans, and procedures, and the deployment of the necessary resources for the security of radioactive material transport. It supports the integration of people, procedures, and equipment through the application of administrative measures. Security management includes measures for access control (to the cargo area, loading and unloading areas, and crew areas of the conveyance), trustworthiness verification, information protection, preparation of the transport security plan, training and qualification of personnel, and event reporting.

For shipments requiring the enhanced security level, a transport security plan should be required for all entities having security responsibilities regarding a shipment. The transport security plan formally documents the responsibilities, procedures, arrangements and security systems that will be used.

The State should establish clear responsibility for, and ownership of, the transport security plan. This will normally be the shipper or carrier having direct responsibility for the security of the radioactive material in any particular mode or phase of transport. In the event that services are subcontracted, it may be appropriate to ensure that contractual arrangements exist to develop and comply with a security plan.

4.3. ESTABLISHING GRADED SECURITY WITH CORRESPONDING GOALS AND OBJECTIVES

Radioactive materials have a wide range of characteristics that make them attractive in varying degrees to adversaries. A corresponding range of effective security measures should be utilized to ensure that the material is adequately protected using the graded approach. Two security levels (basic and enhanced) have been developed to allow specification of security system performance in a graded manner. In cases where the threat or attractiveness of the material warrants more stringent security, or when an alternative categorization method has been implemented (see sections 3.1 and 3.2), the "additional security measures" should be added as the State believes necessary (see Section 5.1.4).

Para. 4.26 of Ref. [5] states that the goal of transport security is to minimize the likelihood of loss of control, or a malicious act. The extent of effort expended to meet this goal (using the graded approach) varies with the threat and security level. This approach supports applying graded security

objectives and measures and takes into account the potential radiological consequences of the radioactive contents.

Malicious acts can involve either unauthorized removal or sabotage. While the security objectives below only address unauthorized removal (i.e. loss of control), achievement of the objectives will reduce the likelihood of a successful act of sabotage. Security systems that achieve the objectives will provide some (although limited) capability to detect and respond to an act of sabotage.

In order to meet the goal, it is necessary to achieve an adequate level of performance for each of the security functions: deterrence, detection, delay, response, and security management. That level of performance is defined as a set of objectives for each of the functions. These objectives state the desired outcome from the combination of measures applied for that objective. Deterrence is a security function which is not possible to measure. Consequently, it has not been assigned an associated set of security objectives and measures in this publication.

Security functions and associated security objectives are summarized in Table 1.

Where an objective is shown in the table as the same for two or more columns, it is intended that the objective be met in a more rigorous manner whenever higher confidence is needed that the security system will prevent unauthorized removal.

TABLE 1. A GRADED APPROACH FOR TRANSPORT SECURITY

<table>
<tr><td rowspan="2">Security Functions</td><td colspan="3">Security Objectives</td></tr>
<tr><td>Basic Security Level
Goal: Confidence that the security system will prevent unauthorized removal</td><td>Enhanced Security Level
Goal: High level of confidence that the security system will prevent unauthorized removal augmented</td><td>Additional Security Measures
Goal: Very high level of confidence that the security system will prevent unauthorized removal</td></tr>
<tr><td rowspan="4">Detection (including assessment)</td><td></td><td colspan="2">Provide immediate detection of any unauthorized access to the package</td></tr>
<tr><td>Provide detection of any unauthorized removal of the package</td><td>Provide detection of any attempted unauthorized removal of the package</td><td>Provide immediate detection of any attempted unauthorized removal of the package</td></tr>
<tr><td></td><td colspan="2">Provide immediate assessment of the detection</td></tr>
<tr><td colspan="3">Verify package count and seal integrity upon delivery</td></tr>
<tr><td>Delay</td><td></td><td>Provide delay that the security system will likely prevent the unauthorized removal</td><td>Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal</td></tr>
<tr><td rowspan="2">Response</td><td>Notify authorities</td><td colspan="2">Provide immediate communication to response personnel and notify authorities</td></tr>
<tr><td>Implement appropriate action in the event of unauthorized removal</td><td>Provide immediate initiation of response to interrupt the unauthorized removal</td><td>Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal</td></tr>
<tr><td rowspan="8">Security Management</td><td>Provide written instructions</td><td colspan="2">Provide a transport security plan</td></tr>
<tr><td colspan="2">Ensure trustworthiness and reliability of authorized individuals, e.g. through background checks</td><td>Consider national security clearance approvals as appropriate</td></tr>
<tr><td>Provide security awareness training</td><td colspan="2">Ensure training and qualification of individuals with security responsibilities</td></tr>
<tr><td colspan="3">Identify and protect sensitive information</td></tr>
<tr><td colspan="3">Provide adequate budget and resources, including a maintenance program</td></tr>
<tr><td>Conduct evaluation for compliance</td><td colspan="2">Conduct evaluation for compliance and effectiveness, including performance testing, exercises and/or drills</td></tr>
<tr><td>Ensure capability to respond to security events</td><td colspan="2">Ensure capability to manage security event covered by the contingency plan</td></tr>
<tr><td colspan="3">Establish security event reporting capability</td></tr>
</table>

In order to achieve the security objectives, the regulatory body should require:

(a) For a performance based approach, a demonstration making it credible that the security measures used will meet the security objectives;

(b) For a prescriptive based approach, specific security measures that must be in place. The regulatory body should satisfy itself that the required measures provide a satisfactory level of security in light of its threat situation. Additionally, some evaluation of the effectiveness of the measures may be needed (e.g., quality of locks, reliability of communications, etc.).

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

This section provides guidance on the content of regulatory requirements to address the security of radioactive material in transport. The regulatory body should satisfy itself that the guidance is incorporated in its regulatory requirements or that decisions have been made to take other approaches in meeting the purpose of the guidance.

5.1. MODE INDEPENDENT PROVISIONS

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

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

This section provides security measures that could be used to protect radioactive material against unauthorized removal or sabotage in transport.

5.1.1. Prudent management practices

Some packages and types of radioactive material are identified in Section 4 as requiring no further security measures other than basic control measures and normal commercial practices. These practices include actions by shippers, carriers and receivers to protect the material against unauthorized removal or sabotage as would be the case for any valuable commodity.

Examples of prudent management practices are:

(a) Securing and storing package while in transport in a manner that impedes unauthorized removal (e.g., in a locked conveyance or storage area);

(b) Utilizing carriers with package tracking systems, e.g. bar code, in place to monitor the status of the shipment;

(c) Using closed vehicles to keep the packages out of sight;

(d) Not leaving packages or conveyances unattended for any longer than is absolutely necessary, for example when deliveries are being made; and

(e) Provide drivers of road conveyances with security training and effective communication equipment.

The material should also be shipped in accordance with applicable dangerous goods regulations, particularly those applicable to radioactive material, and additional requirements for classification, packaging, shipping papers, marking and labelling will apply. These requirements inform carrier personnel of the need to handle and transport the packages with due care and diligence, providing a graded level of protection against unauthorized removal or sabotage.

5.1.2. Basic security level

The guidance in this sub-section applies to all packages of radioactive material defined in Section 4 as requiring at least the basic security level.

At the basic security level measures should include requiring that shippers, carriers, receivers and others engaged in the transport of radioactive material implement graded security systems or other arrangements to deter, detect, delay and respond to malicious acts affecting the conveyance or its cargo. These arrangements should be operational and effective at all times and include training and regular briefings to maintain awareness and vigilance.

5.1.2.1 Evaluation and exchange of security related information

Shippers, carriers and receivers and others engaged in the transport of radioactive material should take into consideration all available threat information, including any threat information provided by the regulatory body, when implementing security measures. For international transport, the threat information for each State involved in such transport should be considered as appropriate.

Shippers, carriers, and receivers should cooperate with each other and with appropriate authorities to exchange information on applying security measures and responding to security incidents, consistent with applicable information protection requirements.

5.1.2.2 Protection and control of security sensitive information

Appropriate measures should be taken to protect sensitive information relating to transport operations, based on a need to know, including information on the schedule and route.

5.1.2.3 Trustworthiness determination

Persons engaged in the transport of radioactive material should be subject to trustworthiness determination by the shipper, carrier, and receiver commensurate with their responsibilities. The trustworthiness determination[2] is a determination of the reliability of an individual, including characteristics and details that may be verified, where legally permitted and where necessary, by means of background checks and by checking criminal records. The trustworthiness determination should be based on background checks of previous activities to verify the character and reputation of the individual. For shipper and receiver personnel, the trustworthiness determination may be the same as that required for their access to radioactive material or sensitive information (including information related to transport activities). Trustworthiness determination is an important element in addressing and controlling insider threats [25].

5.1.2.4 Written instructions, procedures, and plans

Carriers should provide appropriate crew members with written instructions on any required security measures, including how to respond to a security incident during transport. At the basic security level, it is generally sufficient for these written instructions to contain no more than basic details of emergency contacts.

5.1.2.5 Security training

Individuals engaged in the transport of radioactive material should receive training, including training in the elements of security awareness.

Basic security awareness training that includes the need for transport security, 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 (when appropriate) commensurate with the responsibilities of individuals and their part in implementing transport security plans.

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

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

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

5.1.2.6 Shipper and carrier credentials

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

5.1.2.7 Receiver and carrier authorization

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

5.1.2.8 Communications

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

5.1.2.9 Open, closed and special conveyance considerations

Unless there are overriding safety or operational considerations, packages containing radioactive material should be carried in secure and closed or sheeted conveyances, compartments or freight containers. However, carriage of packages weighing more than 2000 kg that are locked and secured to the conveyance may be transported on open vehicles. Whenever it is necessary to use open conveyances, the load should be covered or hidden from view unless safety requirements preclude this. The integrity of the locks and seals should be verified before dispatch, before leaving any stopping point on- route and on arrival by staff specifically and previously authorized to undertake this verification.

5.1.2.10 Conveyance inspections

Carriers should perform security inspections of conveyances, at a frequency commensurate with the material transported, to verify that security measures associated with the conveyance are effective. In

normal circumstances, and as appropriate to the mode of transport, it will be sufficient for the carrier to carry out a visual inspection of the conveyance to ensure that nothing has been tampered with and that nothing has been affixed to the package or conveyance that might affect the security of the consignment. Such inspections may be performed by transport personnel using their own knowledge of the conveyance.

5.1.2.11 Package and conveyance security systems

The package should incorporate a feature which, while intact, will be evidence that it has not been opened. Seals required by the transport safety regulations are generally sufficient. The integrity of seals should be verified before dispatch and on arrival.

5.1.2.12 Monitoring and tracking the shipment

The status of radioactive material in transit should be monitored appropriately. At the basic security level, it is sufficient to use a simple monitoring system such as a package tracking system that can determine when a shipment has departed, when it is in transit, and when the consignment has been received. The information about status changes should be readily available to the appropriate parties (e.g. carriers, shippers and receivers).

5.1.2.13 Continuity of security measures

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

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

When radioactive material is stored in transit, such as in warehouses, and marshalling yards, appropriate security measures should be applied to the material, consistent with the measures applied during use and storage.

5.1.2.14 Receipt verification

The receiver should have procedures in place to verify package contents, which include notification of the shipper and/or carrier in the case of missing radioactive material or when a package has not been delivered by the expected time.

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

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

5.1.3. Enhanced security level

The guidance in this sub-section applies to packages of radioactive material with contents meeting or exceeding the activity threshold for the enhanced security level as defined in Section 4.The measures in this sub-section should be applied in addition to those for the basic security level.

5.1.3.1 Protection and control of security related information

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

See Ref [26] Security of Nuclear Information for additional guidance.

5.1.3.2 Written instructions, procedures, and plans

All shippers, carriers, receivers and others engaged in the transport of radioactive material packages requiring the enhanced security level should develop, adopt, implement, periodically review as necessary and comply with the provisions of a transport security plan.

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

(a) Specific allocation of security responsibilities of organizations and persons engaged in the transport of radioactive material, with appropriate authority to carry out their responsibilities;
(b) Provision for keeping records of radioactive material packages or types of radioactive material transported;
(c) Review of current operations and assessment of vulnerability, including intermodal transfer, storage in transit, handling and distribution as appropriate;
(d) Clear statements of protective measures, including: training, policies including response to conditions of a higher level threat, verification of new employees and employment, operating practices (e.g. choice and use of routes where known, use of guards, access to radioactive material packages requiring the enhanced security level in temporary storage, proximity to vulnerable infrastructure), equipment and resources that are to be used to reduce security related risks;
(e) Effective procedures and equipment for timely reporting and dealing with security related threats, breaches of security or security related incidents (e.g., contingency plans);

(f) Procedures for evaluating and testing security plans and procedures for periodic review and update of the plans;

(g) Measures to protect sensitive information;

(h) Measures to ensure that the distribution of sensitive transport information is limited, to maintain security of the information. Such measures should not preclude the provision of transport documents and shipper's declaration as required by the applicable dangerous goods regulations;

(i) Measures to monitor the location of the shipment;

(j) Where appropriate, details concerning agreements on the point of transfer of responsibility for security.

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

Shippers and carriers should develop and implement a contingency plan to ensure that there would be an adequate response to malicious acts. The contingency plan may be incorporated into the TSP.

5.1.3.3 Shipper and carrier identification

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

5.1.3.4 Receiver authorization

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

5.1.3.5 Planning and coordination

Security during transport should include prior agreement for security functions among the shipper, receiver and carrier. Such agreements may be based on normal commercial practices and responsibilities. For example, agreement should exist on the time and place for transfer of the material, such as when the shipment is released to the carrier and when the shipment is delivered to the receiver.

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

Prior to commencement of transport, the receiver should confirm ability and readiness to accept delivery at the expected time and should notify the shipper on receipt or non-receipt within the expected delivery time frame.

5.1.3.6 Communications

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

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

5.1.3.7 Open, closed and special conveyance considerations

Where practicable, locks and seals commensurate with the categorization of the radioactive material being transported should be applied to conveyances, compartments or freight containers. Locks and/or seals should be checked before dispatch, after any stops made during the journey and during any intermodal transfer of each radioactive material consignment to confirm the integrity. When enclosed freight containers are used, verification of the integrity of a door seal should be sufficient in lieu of verifying each individual seal on packages inside the freight container. Lock fittings and components, such as attachment points and tie downs, should be complementary to the quality and strength of the required locks.

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

When appropriate, electronic intrusion detection and alarms, including duress alarms, should be considered.

Electronic intrusion detection technologies may be suitable for providing immediate indication of when intrusion into the cargo area has occurred. Examples of this technology include: balanced magnetic door switches; light sensors (for closed conveyances); fibre optic and other electronic seals; and passive infrared, microwave or video motion detection.

5.1.3.8 Monitoring and tracking the shipment

As the regulatory body has determined to be appropriate, automated electronic tracking methods should be used to monitor the movement of conveyances containing radioactive material, for example using GPS-based position tracking of the conveyance.

5.1.3.9 Pre-shipment security verification

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

5.1.4. Additional security measures

In certain circumstances, the regulatory body may consider requiring additional security measures in view of the current threat level, the DBT/ATS, or the physical/chemical form and quantity of the radioactive material being transported. For example, the regulatory body may require additional security measures for high activity shipments, such as those exceeding 1000 D. In such cases one or more of the following measures should be considered in addition to those identified in sub-sections 5.1.2 and 5.1.3 to be applied. This list is not exhaustive.

5.1.4.1 Trustworthiness determination

Consideration may be given to subjecting persons engaged in the transport of radioactive material to more stringent trustworthiness procedures, such as national security clearance approvals commensurate with their responsibilities.

5.1.4.2 Written Instructions, Procedures, and Plans

Approval of the transport security plan by the regulatory body may be required, including approval of any required additional security measures.

The contingency plan may be reviewed to ensure that there would be an adequate response to malicious acts. In particular, coordination with response forces should be reviewed to ensure an appropriate and timely response to a malicious act.

Exercises may be carried out to ensure that the transport security and contingency plan are adequately evaluated and tested. If the exercises indicate a need for revisions to the transport security or contingency plan, these should be completed and approved by the regulatory body, as required, before a shipment is undertaken.

Exercises may be limited to arrangements controlled by the shipper and/or carrier or they may also include State level response arrangements.

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

5.1.4.3 Security training

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

5.1.4.4 Shipper and carrier licensing

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

5.1.4.5 Advance notification

Advance notification may be required from the shipper and/or carrier to the regulatory body or other competent authorities. Such advance notification may include details of the shipment, including a description of the material being shipped, planned routes, estimated departure and arrival times, and border crossings as applicable.

5.1.4.6 Communications

Consideration may be given to requiring a transport control centre or other designated point of communication as a central location to monitor and coordinate voice and/or digital communication, to monitor positional tracking, and to facilitate command and control.

Security measures may include provision of continuous two-way voice communication between the conveyance, any guards accompanying the shipment, response forces, the transport control centre, and, where appropriate, the shipper and/or receiver.

Consideration may be given to requiring that secure communications are used during the transport and that such measures provide redundancy of systems. The use of duress codes to initiate response may be considered.

5.1.4.7 Open, closed and special conveyance considerations

Consideration may be given to using conveyances that are specially designed or modified to provide additional security features, for example, a specially designed trailer that allows securing the package to the trailer so that it is not easily removed.

Vehicle disabling devices may be considered. These may include capabilities to disable the vehicle when parked as well as when it is in motion (controlled shut down).

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

5.1.4.8 Conveyance inspections

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

Prior to commencing transport, the carrier should verify that all security measures are in place and are functioning normally in accordance with the transport security plan.

5.1.4.9 Monitoring and tracking the shipment

Consideration may be given to requiring a transport control centre or other designated point of communication as a central location to monitor the shipment, including positional tracking.

5.1.4.10 Guards and individuals accompanying the shipment

Guards may be required to accompany certain shipments to provide for continuous surveillance of the conveyance. The guards should be adequately trained (especially if they are armed), suitably equipped and fully prepared to fulfil their responsibilities.

Additional persons may be required to accompany the conveyance in order to maintain surveillance and control during transport and planned or unexpected stops. The additional individual may be a second driver or crew member.

5.1.5. Overview of security measures

Table 2 provides an overview of the security measures listed in Sections 5.1.2, 5.1.3 and 5.1.4.

TABLE 2. OVERVIEW OF SECURITY MEASURES

		Basic level	Enhanced level	Additional measures
1.	Evaluation and exchange of security related information	5.1.2.1		
2.	Protection and control of security related information	5.1.2.2		
			5.1.3.1	
3.	Trustworthiness determination	5.1.2.3		
				5.1.4.1
4.	Written instructions, procedures, and plans	5.1.2.4		
			5.1.3.2	
				5.1.4.2
5.	Security training	5.1.2.5		
				5.1.4.3
6.	Shipper and carrier credentials	5.1.2.6		
			5.1.3.3	
				5.1.4.4
7.	Receiver and carrier authorization	5.1.2.7		
			5.1.3.4	
8.	Planning and coordination		5.1.3.5	
9.	Advance notification			5.1.4.5
10.	Communications	5.1.2.8		
			5.1.3.6	
				5.1.4.6
11.	Open, closed and special conveyance considerations	5.1.2.9		
				5.1.4.7
12.	Conveyance inspections	5.1.2.10		
				5.1.4.8
13.	Package and conveyance security systems	5.1.2.11		
			5.1.3.7	
14.	Monitoring and tracking the shipment	5.1.2.12		
			5.1.3.8	
				5.1.4.9
15.	Guards and individuals accompanying the shipment			5.1.4.10
16.	Pre-shipment security verification		5.1.3.9	
17.	Continuity of security measures	5.1.2.13		
18.	Receipt verification	5.1.2.14		

5.2. MODE SPECIFIC PROVISIONS

In addition to the mode independent provisions mentioned in Section 5.1, the following provisions should also be considered depending upon the mode or modes of transport to be used in the shipment.

5.2.1 Provisions for road, rail and inland waterway transport

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

5.2.2. Provisions for road transport

The carrier should maintain continuous attendance of the road conveyance during transport where possible. Where non-attendance is unavoidable, the road conveyance should be secured such that it complies with the criteria of protection, detection and response and preferably in a well illuminated area.

If a road movement cannot be completed without overnight or extended stops, then the radioactive material should be protected during such stops in a manner that duly protects the material against malicious acts, according to a graded approach. Security requirements for radioactive materials within a facility might be taken as a basis for defining security requirements during transit.

5.2.3. Provisions for rail transport

If a rail movement cannot be completed without overnight or extended stops, then the radioactive material should be protected during such stops in a manner that duly protects the material against malicious acts, according to a graded approach. Security requirements for radioactive materials within a facility might be taken as a basis for defining security requirements during transit.

5.3. PORTABLE AND MOBILE DEVICES

Portable and mobile device means a piece of equipment containing radioactive material that can be carried by hand or is either mounted on wheels or casters, or otherwise equipped for moving without a need for disassembly or dismounting, or designed to be hand carried.

The ease of handling and concealment of these devices makes them vulnerable to unauthorized removal and attractive to potential adversaries.

For these reasons, specific security measures may be needed in order to account for their portability, for example, by requiring two independent physical barriers to secure radiographic devices during transport.

5.4. PROTECTION AGAINST SABOTAGE

The State's nuclear security regime for radioactive material should include protection against sabotage of the radioactive material, associated facilities and associated activities (including during transport) (Ref. [5], para. 2.1). In fulfilling the recommendation to protect radioactive material during transport, the State should identify the criteria that define what constitutes radiological consequences sufficiently high to warrant protection against sabotage. These criteria may be specified in terms of:

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

An evaluation of the potential for sabotage during transport and a determination of the associated potential radiological consequences may be required by the competent authority. This should be done in close consultation with safety specialists since the transport packaging required for safety purposes may also provide significant protection. Protection against sabotage needs to be implemented with consideration to the measures for safety and against unauthorized removal.

5.4.1. Threat assessment

The State should assess known and potential threats to radioactive material transport with consideration of an adversary's intent and capability to commit acts of sabotage. The objective of sabotage against a radioactive material shipment is the release of radioactive material in sufficient quantity to produce serious radiological harm which could lead to significant socio-economic consequences to the State or the industry. However, even an act of sabotage that is not successful in releasing material or causing radiological consequences may achieve some aspects of those goals.

States utilizing a DBT may consider issuing a specific DBT related to sabotage. The DBT for sabotage is likely to have the same assumptions regarding means and capability of potential adversaries as does the DBT for unauthorized removal. The primary difference in the threat will be seen in the development of scenarios. Additional information on threat assessment and DBT can be found in Ref. [21].

There are many potential sabotage modalities that could be considered and combined in the VA for an attack on radioactive material shipments. These might include projectiles, shaped charges, high explosive modes, high intensity thermal modes or intentionally caused severe incidents. Some of these modalities are relatively high tech and might not be within the scope of the threat defined by the State. Others may require a relatively large number of persons to execute that also may be beyond the

capabilities of the threat. In any case, a realistic evaluation of potential threats and their capabilities is an important aspect in undertaking a vulnerability assessment.

5.4.2. Development of specific threat scenarios

A DBT for sabotage should incorporate the peculiarities of actions and scenarios that are likely to be followed by saboteurs. In particular, a theft or removal scenario mostly comprises two phases: the first phase consists of obtaining access and control of the material while the second phase addresses the adversary's escape with the material. In contrast, sabotage is limited to one phase: defeating the protection of the material by means of weapons or intrusive tools and thereby creating an in-situ radiological hazard to the population or to the environment.

Sabotage scenarios reflect the capability of the threat as determined by the State's intelligence information. One aspect of a scenario is the size of the adversary force, combined with the extent of their training and experience. A second aspect is the attack methods or modalities they can bring to the scenario to achieve the sabotage objective.

5.4.3. Target identification and ranking

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

5.4.4. Estimating the consequences of sabotage considering the threat and the targets

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

In estimating the potential effects of sabotage, safety features of the package and conveyance as well as measures to prevent unauthorized removal should be taken into account with regards to the sabotage threat that includes both the scenario and the mode of attack. The structure of the conveyance and the radioactive material packaging will provide some protection for the material. The degree of protection provided varies with the material being transported and the robustness of the packaging required for safety purposes.

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

(a) Damage due to the blast of the explosive (generally limited to a few hundred metres);

(b) Dispersion of large particles or pieces of radioactive material (generally limited to a few hundred metres);

(c) Airborne dispersion of smaller particles including respirable particles (these can be carried thousands of metres depending on the buoyancy of the plume created by the blast, and accompanying fires).

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

(a) Direct radiation dose from unshielded material that is localized (like an unshielded sealed source);

(b) Direct radiation dose from dispersed material;

(c) Internal radiation dose from airborne material that is generated by the event or material that is re suspended after deposition, or ingested from food or water contaminated by the release from the sabotage event.

In the most basic terms, the severity of radiological impact is directly linked to the source term released to the environment where people can receive a radiation dose directly or where radiation from the deposited material would prevent normal social and economic activity. Thus, the two principal determinants of the quantity released from a shipment subjected to sabotage are:

(a) Package or shipment radionuclide content; and

(b) Fraction of the contents potentially releasable as a result of the sabotage event.

The potential activity release determined by the analysis should be compared to the threshold determined by the State as when additional protection is required. If the threshold defined by the State is based on dose or dose rate, this information should be calculated from the potential activity release, taking into account the radionuclides and form of the material released.

If the calculations show that the sabotage could result in radiological consequences that exceed the State's defined threshold, then additional protective measures, above those required to protect the material against unauthorized removal, may be necessary. The degree to which the calculated results exceed the State's threshold will be one of the principal determinants of the amount of effort taken to minimize the potential radiological impacts of a successful sabotage event. The shipment contingency plan should also be reviewed to ensure that it adequately addresses actions to respond to sabotage initiated situations.

Alternately, it may be possible to add some additional protection features to the transport package or its conveyance to limit the projected release to an acceptable value.

5.4.5. Defining security measures for protecting against sabotage

If the current or potential threat warrants additional security measures to protect against sabotage, consideration should be given to:

(a) Postponing the shipment;
(b) Rerouteing the shipment to avoid high threat areas;
(c) Enhancing the robustness of the package or the vehicle;
(d) Enhancing route surveillance to observe the current environment;
(e) Providing guards or increasing the number of guards.

When establishing security measures to protect against a malicious act, particularly sabotage, the safety features of the design of the transport package, container and conveyance should be taken into account.

5.4.6 Applicable security measures

A wide variety of materials and concepts could be applied to existing packagings in order to minimize release of radioactive materials to the environment in the event of an attack on a shipment. Several of these features also have application to preventing unauthorized removal of the material by increasing the time needed to retrieve the material from the packaging.

Both active and passive delay features are possible. Measures to be taken could include protecting against an attack device being placed close to the package/conveyance, such as protective metal covers. Conveyances transporting spent fuel cask may be fitted with covers that can reduce the effectiveness of explosives and reduce penetration abilities of stand-off attacks. Masking covers such as soft sided rollback trailer covers can be used to prevent direct visual observation of the package.

Most of the measures will impact the operation of the transport system due to additional procedures required in the preparation of a shipment; however, the measures should not adversely affect the safety of the package.

5.4.7. Applicable organizational measures

During loading and unloading and transhipment when packages are removed from their conveyances, the State should consider the need for compensatory protective measures such as additional guards, barriers and surveillance. Additional inspections prior to movement can also be made to ensure that nothing has been attached to the package, container or conveyance that could cause damage.

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

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

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

6.1. STATE RESPONSIBILITIES

The State should ensure within its regulatory framework that roles and responsibilities are clearly defined in the event that radioactive material is determined to be lost, missing, misplaced or stolen during transport. Procedures should be established to ensure that information and assistance is available to support rapid and comprehensive measures to locate and recover missing or stolen radioactive material.

Shippers, carriers and receivers should be required to notify the regulatory body within a specified time of any radioactive material that is determined to be lost, missing, misplaced or stolen during transport. Once a package with radioactive material has been reported to be lost, missing, misplaced or stolen during a transport, the situation is then out of the shipper's or carrier's control. The State should therefore implement the recommendations in the IAEA Nuclear Security Series Number No.15, Nuclear Security Recommendations on Nuclear and Other Radioactive Materials out of Regulatory Control [11].

The State should ensure that national-level contingency plans are established for the actions it will take to locate and recover any radioactive material that is reported as missing or stolen during transport. These contingency plans should be coordinated with emergency response plans [13, 14].

6.2. SHIPPER, CARRIER AND RECEIVER RESPONSIBILITIES

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

Upon discovery that a package has been lost or removed from a conveyance, the carrier should initiate an immediate search to determine if the packages may have been inadvertently misplaced and remain under its control. As good practice, the carrier may wish to notify the competent authority upon suspicion of loss, unauthorized removal, or tampering of a package. If loss of control is confirmed, the carrier should notify the relevant authorities as well as the shipper. Additionally, the carrier should provide assistance with all efforts to locate the packages (i.e. tracing previous movements and handling transactions, providing requested information) and should fully cooperate during any subsequent investigations and/or prosecutions.

If the carrier locates the missing package(s) after it has notified the authorities and the shipper of an incident, the carrier should promptly inform them that the package(s) have been found.

APPENDIX I. SETTING SECURITY LEVELS

I.1. MALICIOUS USE OF RADIOACTIVE MATERIAL

Potential malicious acts involving radioactive material cover a wide spectrum of possible scenarios. The following events represent some broad categories of possible malicious acts with the potential to give rise to significant radiological consequences:

(a) Covert placement of unshielded material in working and/or living areas or street locations where the public might be externally irradiated.

(b) Sabotage of radioactive material packages or shipments with the subsequent release of radioactive material and its dispersal to the environment.

(c) Capture of a radioactive material package or shipment and the subsequent dispersal of the material by means of conventional explosives. The main radiological consequences from such an event, i.e. an RDD scenario, include both near-field and far-field effects. In the vicinity of the explosion (near-field) there may be radioactive shrapnel and larger pieces of radioactive material dispersed in the area and injuring persons and damaging and contaminating buildings, etc. and also general contamination from vaporized or finely divided material. Persons in the area may inhale vaporized or finely divided material and their skin and clothes may be contaminated. There may also be a rising plume that disperses vaporized and finely divided material (to the far-field) resulting in contamination of the area and of persons in the area, as well as exposure due to inhalation as the plume passes.

(d) Capture of a radioactive material package or shipment and its subsequent processing (e.g. transformation into a more highly dispersible form) with subsequent dispersal of the radioactive material in the environment (RDD scenario). The time and resources required for this action would increase the likelihood of successful intervention by security forces, so this scenario is considered less likely than others.

The radiological consequences arising from radiological attacks of these types are extremely variable depending on, for example, the type and nature of the event and the type and amount of radioactive material involved. Since the RDD scenario may be a very attractive means for adversaries to cause harm and can be undertaken with unsophisticated capabilities, it is considered a more likely scenario. The RDD scenario is also considered appropriate in respect of evaluating the potential radiological consequences of a malicious act involving different radionuclides.

I.2. ESTABLISHING SECURITY LEVELS

Since the transport of radioactive material occurs within the framework of the transport of other dangerous goods, it is desirable to be as consistent as possible with existing security requirements and

guidelines, particularly the UN Model Regulations [4] and the international modal regulations [6, 7]. Additionally, since some radioactive material is also covered by the Code of Conduct [19] with its supplementing guidance, the CPPNM [16] together with its Amendment [27] and NSS No. 13 (INFCIRC/225/Rev.5) [17], it is also desirable to be as consistent as possible with these documents. The security levels included in this publication have been developed with these considerations in mind.

Since transport operations vary widely in how they are carried out (whether full load, consignments of individual packages, etc.), it is necessary to clearly define the basis for specifying security measures. There are three feasible bases for specifying what should be subject to enhanced transport security measures:

(a) Per package: enhanced security provisions would be applied when any package in a consignment exceeds the threshold value. There are operational benefits to this approach, such as not requiring carriers to keep a tally of the total activity on the conveyance. However, this approach may not provide an accurate measure of the potential harm that a single diverted conveyance could be used to cause (since multiple packages could be present on a single conveyance).

(b) Per conveyance: enhanced security provisions would be applied when the total activity on a conveyance exceeds the threshold. This approach ensures that the total activity on a single conveyance will not exceed the threshold without necessitating the enhanced security provisions. However, this would be difficult to implement operationally, particularly for international shipments and those transported by aircraft or vessel where many consignments from a variety of shippers may consolidated.

(c) Per consignment: A consignment consists of the package(s) presented for transport by a shipper at one time to a carrier. This approach results in aggregating the total activity offered by a shipper at one time and does not require the carrier to keep a tally of the total activity on the conveyance. However, multiple consignments from multiple shippers could still be accepted by the carrier which could exceed the threshold value without triggering the enhanced security provisions.

The per package approach is used in this publication for specifying the security level. States may wish to consider either the per conveyance or per consignment approach for domestic transport by vehicle but a per package approach is recommended for international transport by all modes.

There are some packages of radioactive material with such low levels of radioactivity that they present low radiological hazards and correspondingly low security risks, e.g. consumer products, very small quantities of radionuclides and material with very low activity concentration. Because of the very limited potential consequences that could arise from their use in malicious acts, certain packages

and materials need not be subjected to transport security provisions more stringent than those ordinarily applied to a commercial shipment. These packages and materials are defined and specified in Ref. [1] and are also identified by their UN number. These packages and materials should meet the activity limits and other specifications contained in Ref. [1] and include:

(a) Empty packagings – UN 2908;
(b) Articles manufactured from natural uranium, depleted uranium or thorium – UN 2909;
(c) Excepted packages with an activity level not exceeding the level permitted for the radionuclide when it is not in special form – UN 2910 and UN 2911;
(d) LSA-I (low specific activity materials) – UN 2912;
(e) SCO-I (surface contaminated objects) – UN 2913; and
(f) Uranium hexafluoride, radioactive material, excepted package, less than0.1 kg per package, non-fissile or fissile excepted - UN 3507.

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

For packages and materials exceeding the activity level allowed in those above listed above, the potential consequences of their use in a malicious act vary greatly (over many orders of magnitude). However, in order to specify appropriate transport security measures, packages may be grouped on the basis of their potential consequences. A small number of security levels are desirable for simplicity, but a larger number of security levels make it easier to 'tailor' the security measures more precisely to the potential radiological consequences of the material. Two security levels are recommended for specifying transport security measures for packages containing more radioactive material than allowed without specific security measures. The use of two levels allows the security measures to be specified as simply as possible while identifying packages that warrant either basic or enhanced security measures.

The use of two levels for security in transport means that some quantitative measure must be used to specify which level is assigned to a package (that is, the criterion). This can be done by defining an activity threshold since the potential consequences of the contents of a package are based on the radionuclides and activity levels in the package. The use of a single activity level threshold is also consistent with the approach to the transport of dangerous goods of the UN Model Regulations [4]. This threshold specifies the criterion for distinguishing between 'high consequence' (UN Model Regulations terminology) radioactive material packages and other radioactive material packages (above the level of excepted packages, LSA-I, and SCO-I which do not warrant security measures beyond prudent management practices).

This approach results in a total of three levels of security in transport for packages which, on the basis of their potential consequences, are subject to:

(a) **Prudent management practices** — consignments consisting of excepted radioactive material packages (with contents not exceeding the activity allowed for the radionuclide(s) in non-special form) and radioactive material specified as LSA-I and SCO-I. No additional provisions other than those control measures required by the Basic Safety Standards [3] and normal commercial practices are suggested.

(b) **Basic security level** — consignments consisting of packages analogous to other dangerous goods subject to the 'General Provisions' for dangerous goods security in the UN Model Regulations [4] (packages that are below the specified activity threshold);

(c) **Enhanced security level** — consignments that include at least one package analogous to 'high consequence' dangerous goods as defined in the UN Model Regulations [4] (i.e. a package that is above the activity threshold).

In certain circumstances **additional security measures** may be considered by a State, see section 5.1.4.

The transport security levels are illustrated in Figure 3.

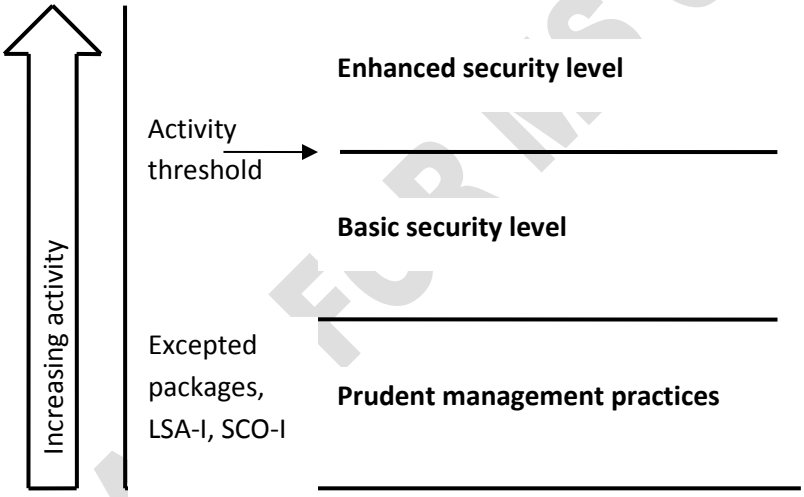

FIG. 3. Incremental transport security levels.

I.3. DEFINING ACTIVITY THRESHOLD

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

Considerable work has been done to define a 'dangerous source', see Ref. [28]. This work identifies exposure scenarios and dose criteria used to define the quantity of a radionuclide that would constitute a danger to an individual (the 'D' value). These scenarios also include a dispersion scenario that may

be relevant to a malicious act. The scenario included dispersal of a source, for example by fire, explosion (i.e. by means of an RDD) or human action, resulting in exposure of an individual due to inhalation, ingestion and/or skin contamination [28].

Recognizing that the Code of Conduct [19] is being implemented by many Member States, the approach embodied in the Code was examined to determine whether it could be used for setting the activity thresholds for the radionuclides included in the Code. Reasonable correlation was found with 1000 D for beta/gamma emitters and 10 D for alpha emitters. Since a radioactive source containing 10 D is 10 times more dangerous than the reference 'dangerous source' and is capable of producing severe deterministic effects, it was decided that a value of 10 D could be used to specify the enhanced transport security level for radionuclides included in the Code.

For radionuclides not included in the Code of Conduct [19] another approach is needed for specifying the activity threshold. A strong desire has been expressed to specify the activity threshold in terms of the traditional transport safety A-values. These values are calculated using the 'Q system' that has been incorporated in the Transport Regulations for over 35 years (see SSG-26, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material [29]).

The A_1 values are derived for special form (non-dispersible) radioactive material and the A_2 values are for 'other than special form' (dispersible) radioactive material. The A-values are not based on exposure scenarios that are appropriate for representing the potential consequences of an RDD. However, they are derived from transport accident scenarios and well established in relation to the transport of radioactive material. Consequently, a multiple of the A-values was considered to be the desired way to express the activity threshold. When the radionuclides covered by the Code of Conduct [19] are disregarded, the remaining radionuclides showed good correlation with a value of 3000 A_2 (since the A_2 value of a radionuclide never exceeds the A_1 value). Subsequently, for radionuclides not included in the Code of Conduct [19], a value of 3000 A_2 may be used to identify packages that are subject to the enhanced transport security measures. This does not mean that 3000 A_2 corresponds to the same risk of causing severe deterministic health effects as 10 D. For some radionuclides, 3000 A_2 is 1000 or more times the quantity of a radionuclide (D value) that, if not under control, could result in severe deterministic health effects to an individual.

I.8. MIXTURES OF RADIONUCLIDES

For mixtures of radionuclides, determination of whether or not the transport security activity threshold has been met or exceeded can be calculated by summing the ratios of activity present for each radionuclide divided by the transport security threshold for that radionuclide. If the sum of the fractions is less than 1, then the activity threshold for the mixture has not been exceeded.

This calculation can be made with the formula:

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

Where:

A_i = activity of radionuclide *i* that is present in a package (TBq)

T_i = transport security threshold for radionuclide *i* (TBq).

I.9. SPECIFICATION OF THE TRANSPORT SECURITY THRESHOLD

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

3000 A_2 in a single package, except for the following radionuclides:

Radionuclide	Transport security threshold (TBq)
Am-241	0.6
Au-198	2
Cd-109	200
Cf-252	0.2
Cm-244	0.5
Co-57	7
Co-60	0.3
Cs-137	1
Fe-55	8000
Ge-68	7
Gd-153	10
Ir-192	0.8
Ni-63	600
Pd-103	900
Pm-147	400
Po-210	0.6
Pu-238	0.6
Pu-239	0.6
Ra-226	0.4
Ru-106	3
Se-75	2
Sr-90	10
Tl-204	200
Tm-170	200
Yb-169	3

APPENDIX II. TRANSPORT SECURITY PLAN

The transport security plan (TSP) documents the security arrangements, personnel and equipment that will be used to provide security during transport.

The State should clearly establish responsibility for and ownership of the transport security plan.

The TSP should be required for transport of radioactive material requiring the enhanced security level or whenever the regulatory body determines that one is necessary.

The entities responsible for having a TSP are normally the shipper, carrier, receiver and any other entities having direct responsibility for the security of the radioactive material in any particular mode or phase of the transport. In the event that transports are subcontracted, contractual arrangements should exist to ensure development and compliance with a transport security plan. Alternatively, subcontractors should be obligated to comply with a transport security plan developed by the contracting entity.

II.1. DEVELOPING THE TRANSPORT SECURITY PLAN

A first step in developing the TSP is an evaluation of potential vulnerabilities for the shipment(s) that will be subject to the TSP. Such an assessment takes into account all information, as appropriate, regarding the mode or modes of transport; inter-modal transfers; the route to be followed; any transit sites, stopover points, temporary storage or transfer areas; conveyances, equipment and personnel; and, planned or potential stopping places. The result of this assessment is then used to make a judgment as to whether the overall effectiveness of the security system is adequate or if improvements such as compensatory measures are needed.

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

All shippers, carriers, receivers and others engaged in the transport of radioactive material should also have contingency plans in place to respond to malicious acts involving radioactive material in

transport, including plans for actions to take for recovery of lost or stolen material and for mitigating radiological consequences of sabotage. These contingency plans may be a separate document or a part of the TSP.

II.2. SUBMITTING AND OBTAINING APPROVAL OF THE TRANSPORT SECURITY PLAN

The State should specify whether a TSP and, if required, any associated vulnerability assessment (VA) needs to be submitted to the regulatory body for review and approval. This may depend upon the category of material being proposed for transport, for example requiring TSPs for both Category 1 and 2 radioactive material shipments but only requiring approval of TSPs for Category 1 shipments. The approval process can also be iterative. If the regulatory body feels that the State requirements are not met in the proposed TSP or that the results of the VA are inadequate, the TSP and/or VA along with a list of the identified shortcomings should be returned to the originator for additional information and revision.

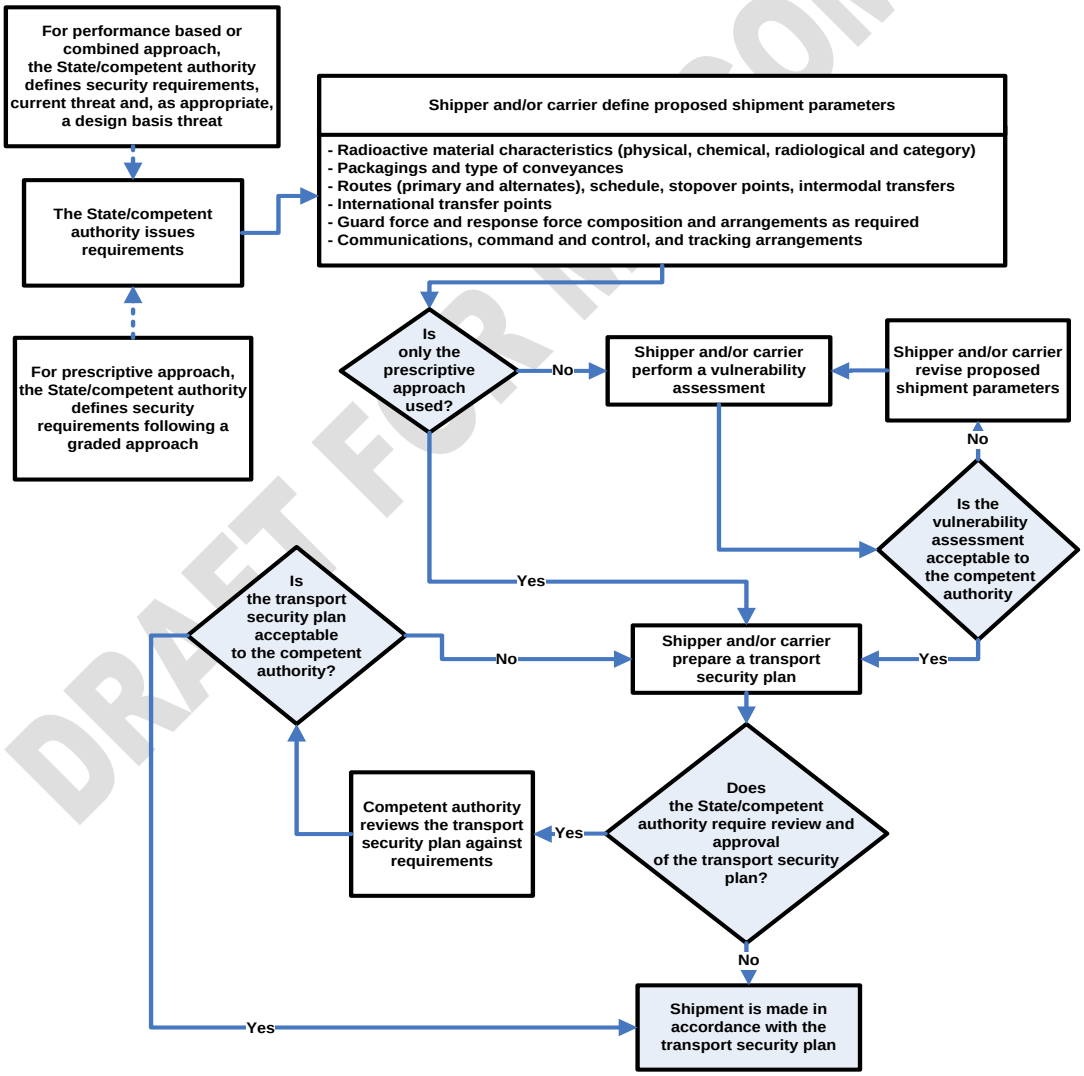

FIG. 4. Sample process for competent authorities' review and approval of a vulnerability assessment, if needed, and a transport security plan.

II.3. IMPLEMENTING THE TRANSPORT SECURITY PLAN

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

After commencing transport, if the shipment cannot be completed in accordance with the TSP the shipper or carrier should immediately implement compensatory measures to maintain the level of protection. If the TSP is one that has been approved by the competent authority, the shipper/carrier should inform the regulatory body as soon as is practicable. The regulatory body may require the shipper/carrier to prepare a set of compensatory measures in advance.

If any incidents or unscheduled delays have occurred during transport, a review of security arrangements should be carried out in order to evaluate the effectiveness of the TSP and to identify any necessary improvements that may be made to optimize its effectiveness for future shipments.

II.4. CONTENT AND ORGANIZATION OF THE TRANSPORT SECURITY PLAN

An example structure of a Transport Security Plan (TSP) is provided below. A State may need to modify this outline to reflect its own particular circumstances, but the example contains the types of information that the State may need in order to validate and approve the proposed security measures and arrangements. States should require this or a similar structure to facilitate understanding between shippers, carriers, receivers, others involved in the transport and regulators both domestically and internationally.

II.5. EXAMPLE OF STRUCTURE OF THE TRANSPORT SECURITY PLAN

1. SCOPE
2. OBJECTIVES
3. DESCRIPTION OF THE SHIPMENT AND MATERIAL TO BE TRANSPORTED
   - 3.1 Description of radioactive material
   - 3.2 Mode(s) of transport
4. ADMINISTRATIVE REQUIREMENTS
   - 4.1. Policies and procedures
   - 4.2. Vulnerability and threat assessment
   - 4.3. Testing and evaluating the transport security plan
   - 4.4. Transport security verification

4.5. Notification of relevant agencies

4.6. Review and update of the transport security plan

5. PERSONNEL QUALIFICATIONS

5.1. Trustworthiness

5.2. Training

6. RESPONSIBILITIES

6.1. Organizational structure

6.2. Allocation and transfer of responsibilities

7. INFORMATION MANAGEMENT

7.1. Information security

7.2. Records retention

8. TRANSPORT SECURITY MEASURES

8.1. Routes

8.2. Transport security system

8.2.1. Conveyance

8.2.2. Operations command and control

8.2.3. Physical protection measures

8.2.4. Communications and positional tracking for normal operations

8.2.5 Maintenance and testing of systems and equipment

9. EMERGENCY RESPONSE

9.1. Emergency and contingency response

9.2 Communications during incidents

9.3 Reporting of threats and incidents

II.6. EXAMPLE OF CONTENT OF THE TRANSPORT SECURITY PLAN

The following sections outline the details that should be considered for inclusion in a TSP for a shipment of radioactive material.

1. SCOPE

This section should define the shipment(s) and entities that are covered in the TSP, including:

— The type of radioactive material to be shipped;

— The locations of the shipper and receiver;

— The identification of the carrier;

— The regulations, requirements that were used in the development of the TSP.

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

2. OBJECTIVES

This section should provide a clear statement of the objectives that the plan is intended to accomplish, including:

— Ensuring security to protect personnel, equipment, radioactive material;

— Providing clear direction to personnel on actions to be taken to:

- Ensure security of shipments; and
- Provide appropriate response to incidents.

3. DESCRIPTION OF THE SHIPMENT AND MATERIAL TO BE TRANSPORTED

3.1. Description of radioactive material

The description of the material to be transported should include:

— Nature of the material;

— Type;

— Quantity (activity);

— Physical and chemical characteristics;

— Category;

— Hazards;

— Packaging;

— Number of packages in a consignment.

3.2. Mode(s) of transport

The mode(s) of transport (road, rail, air, water) should be specified.

4. ADMINISTRATIVE REQUIREMENTS

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

4.1. Policies and procedures

This section should list those specific policies and procedures, issued either by State entities or the responsible party, that apply to the shipment(s). Specifically:

— Policies and operational procedures for consistent implementation of security measures addressed in the Transport Security Plan.

— Contingency plans for responding to malicious acts during transport, recovery of lost or stolen material, and mitigation of consequences.

4.2. Vulnerability and threat assessment

This subsection should elaborate on how the shipper and/or carrier will ensure security measures are adequate by performing a vulnerability assessment that accounts for the threat level.

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

The threat level used should be described and a description of how threat level changes will be communicated and acted upon should be included. Changes in the transport environment that may require evaluating the need for operational changes should be identified, such as activities that might impact routeing (e.g., activists/demonstrations, road conditions, traffic conditions, secure parking for overnight trips).

4.3. Testing and evaluating the TSP

The TSP should specify the procedures for evaluating and testing its effectiveness.

4.4. Transport security verification

This subsection should elaborate on how the shipper and/or carrier will ensure that all specified security measures are present and operational prior to initiating a shipment. Any planned use of checklists for performing the pre-shipment verification and any corrective actions should be outlined.

4.5. Notification of relevant agencies

The plan should clearly specify the responsibility for, timing of, and method of communicating notifications to relevant agencies (before, during and/or after transportation).

4.6. Review and update of the TSP

TSPs should be reviewed periodically to ensure it is up to date and that the latest available threat information has been taken into account. Because the TSP should be reviewed periodically, it should specify when and how the reviews and updates are to be accomplished.

5. PERSONNEL QUALIFICATIONS

5.1. Trustworthiness

The level of trustworthiness required for personnel involved in the transport should be described and should be commensurate with their security responsibilities. The process used to verify trustworthiness at each of those levels should be described.

5.2. Training

This section of the TSP should identify training requirements for personnel involved in the transport. It should specify the nature and frequency of the training.

A description of any exercises that will be conducted should be included as well as the schedule that will be followed for each type of exercise. A description should be included of how the results of exercises will be evaluated, including documenting the results of the exercises and any corrective actions taken.

6. RESPONSIBILITIES

This section should elaborate on how responsibilities are assigned and how they are transferred as shipments proceed.

6.1. Organizational structure

The organizational structure of the entities involved in the transports should be specified, describing the chain of command including names of responsible personnel.

6.2. Allocation and transfer of responsibilities

The responsibilities of all organizations and persons engaged in the transport of radioactive material should be described, including how and when security responsibilities are transferred.

7. INFORMATION MANAGEMENT

The manner by which all information will be managed should be specified in this section, particularly for security sensitive information. Reference to other information management procedures may be used.

7.1. Information security

This section should describe how security of information will be ensured. This description may include: identification of sensitive information, classification review and marking, reproduction restrictions, distribution (authorized access; need-to-know), storage requirements and destruction.

7.2. Records retention

This section should identify who has responsibility for retaining records to ensure required records are handled in accordance with regulatory requirements and procedures (may include requirements for shippers, carriers, and receivers).

8. TRANSPORT SECURITY MEASURES

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

All sensitive information should be handled according to procedures that are outlined in Section 7 of the TSP.

8.1. Routeing

The routes, and associated in-transit storage and inter-modal transfer locations should be specified. Information should include:

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

8.2. Transport security system

This sub-section should describe the security system, including specific security measures (based on the security level of the shipment) and other arrangements that will be used.

8.2.1. Conveyance

The conveyances (road, rail, air, water) should be specified, including any special requirements for the conveyances.

8.2.2. Operations command and control

Command and control procedures should be clearly identified for normal and emergency operations. This information should include chain of command structure, decision making authority, points-of-contact and identification of response agencies.

8.2.3. Physical protection measures

The physical protection measures to be used during transport should be identified. These should include measures used to provide detection, delay and response. Examples of these measures include:

- Tamper indicating devices and seals (packages and conveyances);
- Locks (single or multiple) for packages, cargo compartment, and conveyance (e.g., door keys, ignition keys);
- Secure tie-downs and over-packs;
- Immobilizing devices.

The process for authorizing alternative measures (such as when a feature is not operational or available) should be identified.

8.2.4. Communication and positional tracking for normal operations

This section should describe the structure of the primary and alternative communication systems for the transport operation. Any system for tracking the conveyances should be described including identification of the location at which shipment monitoring will occur.

8.2.5. Maintenance and testing of systems and equipment

This section should address how all of the systems involved in the shipment(s) (such as communications and tracking) are maintained and tested.

The section should also address the checking and testing of all mission-related equipment that will be performed prior to the beginning of the transport. Periodic testing requirements should be specified.

9. EMERGENCY RESPONSE[3]

Emergency response includes both tactical and non-tactical (i.e., non-security related emergency) planning. In this section, the range of incidents that might require response should be identified, the appropriate response measures should be described, and the response resources should be clearly defined.

9.1. Emergency and contingency response

This section should identify how responses to emergency and security-related incidents will be handled. Response actions should include what actions will be by crew members, the transport control centre or other operations centre, shipper and/or receiver technical support staff, emergency response units along the route, escort personnel (if present), guard or security force (if present), and response forces.

Emergency situations may include road closure, vehicle breakdown, vehicle accidents and driver illness. Corresponding emergency arrangement may include but are not limited to availability of backup vehicles and drivers, capabilities for towing and lifting and plans for use of safe havens.

Any required advance information to response forces along the route should be described, including the time frame in which it should be completed prior to the shipment.

Any accompanying guard or security force should be identified.

9.2. Communications during incidents

A description of the communications systems and actions that will be taken to address both emergency and nuclear security events should be included. This information may include the types of communications equipment used and features to ensure the security of communications.

9.3. Reporting of threats and incidents

Reporting requirements should be described, including types of events that require reporting, to whom and how the event will be reported and the timeframe for reporting.

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

APPENDIX III. TRANSPORT SECURITY VERIFICATION

The transport security verification is a mechanism that can be used to identify any deficiencies prior to making a shipment of radioactive material. The verification process may be coupled with identifying and completing corrective actions which can result in confidence that the planned security level is provided.

Shipment security verification should be performed in stages. The first stage (referred to as "security arrangement verification" in the table below) should occur well in advance of shipments, to ensure deficiencies are identified and time is available to resolve them. A final verification just prior to departure (the "pre-shipment verification") should also be completed to ensure that all security measures called for in the TSP are in place and operational. The number and extent of verifications can follow a graded approach, and also be determined based on past history of, and experience with earlier shipments.

The table below presents security features that should be verified for a shipment by road. If transport by means other than road is to be undertaken, the table will need to be appropriately modified.

The table may be useful for shipper/carrier self-assessments, security audits and inspections by the regulatory body. The user may wish to use the table below to inform their development of verification checklists specific to their own operations.

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

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

	Security arrangements verification	Pre-shipment verification
Does the security plan specifically allocate responsibilities?		
Does the security plan provide for the keeping of records of radioactive material packages or types of Class 7 radioactive material transported?		
Does the security plan provide for review of current operations and assessment of vulnerabilities?		
Does the security plan provide clear statements of security measures and procedures that will be followed?		
Does the security plan clearly specify, consistent with guidance from the State, who or what organization is responsible for the plan?		
Policies and Procedures		
Is a list of all relevant policies and procedures available, and are these policies and procedures known to be available to all personnel to whom they apply?		
Testing and Evaluation of the Security Plan		
Has there been any testing of the security plan, under the direction of the Transport Security Manager, or its designee, with company employees, contractors, carriers, or other affiliated parties?		
Have drills and exercises related to the relevant Radiological Accident Emergency Plan been performed? (required at least annually)		
Has the Transport Security Manager, or its designee determined the need for and scheduling of a security or emergency response drill or exercise related to this plan?		
Were the specified security or emergency response drills or exercises undertaken, and were the results thereof properly documented in accordance with relevant quality assurance requirements?		
Has the transport vehicle been visually inspected by personnel designated by the Transport Security Manager, or its designee prior to departure from the shipper's facility to ensure that nothing has been tampered with and that nothing has been affixed to the packages or the transport vehicle which might affect the security of the shipment?		
Are any in-transit shipment inspections required?		
Review and Update of the Security Plan		
Has the Transport Security Manager, or its designee, performed a pre-shipment review of the plan immediately prior to any applicable shipment to ensure no immediate changes are required?		
What organizations and personnel participated in the review?		
Vulnerability Assessment		
Has the Transport Security Manager, or its designee received information that a threat level, elevated above the previous threat level evaluated, exists such that appropriate actions to revise security measures in this plan need to be implemented?		
What steps were taken to address any change in threat level? (Please describe as needed)		
Immediately prior to each shipment, has the Transport Security Manager, or its designee reviewed the planned transport operations and assessed vulnerabilities considering critical factors, including (but not limited to) the following factors: {Check the factors below that have been assessed}		
• equipment operability,		
• schedule,		
• weather, and		
• routes to be followed and any potential alternate routes, such that adjustments to the plan are necessary?		
• Other (specify)		
Threat Assessment		
Have any threat, emergency, delay in transit, unusual situation, or incident for any onsite movement or offsite shipments of "high consequence" radioactive material been identified or reported?		

	Security arrangements verification	Pre-shipment verification
If any threat, emergency, delay in transit, unusual situation, or incident for any onsite movement or offsite shipments of "high consequence" radioactive material has been identified or reported, has it been reported to the appropriate personnel and authorities? (Specify details regarding what actions were taken as a result of the event that caused the reporting.)		
Reporting of Threats and Incidents		
Are all personnel involved in the shipment aware that any threat or incident should be reported immediately to appropriate management personnel?		
Are methods for reporting threats and incidents specified in procedures?		
3. PERSONNEL-RELATED ELEMENTS		
Allocation and Transfer of Responsibilities		
Are procedures and documentation available to properly control the allocation of responsibilities among involved personnel (include establishing commensurate authorities).		
Are procedures and documentation available to properly control the transfer of responsibilities as follows?: (a) Between shipper and carrier (b) Between carriers (if applicable) (c) Between carrier(s) and interim storage sites (if applicable) (d) Between carrier(s) and intermodal transfer facilities (if applicable) (e) Between carrier and receiver		
Organizational Structure		
Has the organizational structure for the shipment been appropriately documented and communicated, including specification of the chain of command and identification of responsible personnel?		
Trustworthiness		
Has the Transport Security Manager, or its designee ensured that personnel involved in shipments of recovered sources are trustworthy by the use of background checks prior to employment, security awareness, and annual assessments of job performance?		
Is positive identification of involved personnel provided through the use of photographic identification badges?		
Training		
Does the training required to be provided to involved personnel include the security measures per this plan?		
Is required training for all personnel involved in the shipment (vehicle drivers, guards, and response personnel) up to date?		
Are training records for all personnel involved in the shipment up-to-date and maintained in accordance with record keeping policies and procedures established by or through the Transport Security Manager, or its designee?		
Have personnel been trained on the methods for reporting threats and incidents?		
4. INFORMATION MANAGEMENT		
Information Security		
If the State requires advanced notification of this shipment to any party, have steps been taken to ensure the security of the information contained in the notification?		
If advanced notification is required, have the organizations to be notified been provided with the required advance notification information?		
Records Retention		
Are all applicable records (including those shown in list below) associated with this shipment permanently retained by the organization designated by the Transport Security Manager, or its designee according to existing policies established by the Transport Security Manager, or its designee?		
(a) Training		
(b) Transport documents (including transport security plan)		
(c) Verification of sources (nuclides, activities and configuration of sources)		
(d) Source information		
a. When received		

	Security arrangements verification	Pre-shipment verification
b. How received		
c. Location of Storage		
(e) Shippers report of:		
a. Transfer of sources		
b. Authorizing signatures in accordance with procedures		
Other (specify)		
Confidentiality and Protection of Information		
Has the Transport Security Manager, or its designee ensured that access to the elements of this plan have been restricted to those who have a need-to-know and that sensitive information in this plan, or otherwise associated with the recovered source shipments, has been handled in accordance with the confidentiality procedures established by or through the Transport Security Manager, or its designee?		
5. TRANSPORT SECURITY SYSTEM		
Primary and Alternate Routes		
Has the Transport Security Manager, or its designee arranged for review and approval, by each affected public security bureau, of the schedule and routes – both primary and alternate routes – that are expected to be followed for the shipment of radioactive sources or radioactive material? (Specify the affected public security bureaus that have reviewed and/or approved)		
Are any in-transit stops anticipated? (If any in-transit stops are anticipated, document the manner by which they have been authorized and are known to be secure.)		
Has the Transport Security Manager, or its designee requested information on any expected delays, detours, road construction, traffic holdups, or weather issues that could delay transit? If information of potential delays in transit has been identified, how has that been incorporated in to the transport security plan?		
Equipment-related elements		
Equipment and Modes of Transport		
Packages: Are features of each of the packages to be transported that are important to the security identified, including at least the following?		
(a) Tamper indicating devices?		
(b) Locks?		
(c) Package identification numbers?		
(d) External radiation levels?		
(e) Others (specify, e.g. any capabilities for deterrence, detection or delay)		
Security measures on packages: Are the following security measures in place for the packages? (specify the measures that are in place)		
(a) tamper indicating device on the packages		
(b) locks on: packages, when included in the design		
(c) locks on package tiedowns (e.g. chains)		
Conveyance:		
Is the conveyance to be used (a) a closed van type, or (b) an open, flat-bed type? [(a)] or [(b)] (specify relevant details in comments column)		
Is the transport vehicle owned by the carrier or is it owned by the shipper or otherwise under the control of the Transport Security Manager, or its designee?		
Does the transport vehicle have incorporated into it any capabilities for deterrence, detection or delay?		
Security measures on conveyance: Are any of the following security measures in place on the transport vehicle? (specify the measures that are in place)		
(a) cargo compartment door of the transport vehicle, if an enclosed van type vehicle is to be used		
(b) ignition of the transport vehicle		
(c) door on the cab of the transport vehicle		

	Security arrangements verification	Pre-shipment verification
Operating personnel: If transport is by road, does the transport vehicle have a driver accompanied by one or two additional appropriately qualified and equipped personnel? (specify the number of accompanying personnel and the manner in which they are qualified and equipped)		
If transport is by road, will each transport vehicle be accompanied by one or more escort vehicles, each carrying two armed or unarmed guard force personnel? (Specify the number of escort vehicles, whether the escorts are armed or unarmed)		
Are all involved personnel instructed to ensure that the tie-downs and, as applicable, the cargo doors of the conveyance are to remain locked whenever the packages are loaded on the conveyance?		
Has the shipper provided appropriate crew members with written instructions on any required security measures, including how to respond to a security incident during transport?		
Have arrangements been made to ensure that the transport vehicle and associated escort vehicles are continuously manned during transit? If continuous attendance is not arranged for, have arrangements been made to secure the vehicles in a manner that complies with the principals of protection, detection and response and preferably in a well-illuminated area?		
Tiedowns: If the package(s) of radioactive sources or radioactive material are contained and carried in a closed vehicle, will the tie-downs and the cargo doors of the conveyance remain locked whenever the packages are loaded on the conveyance?		
If the package(s) of radioactive sources or radioactive material are carried on an open, flat-bed vehicle, will the tie-downs remain locked whenever the packages are loaded on the conveyance?		
Locks: Has the integrity of all locks been verified prior to dispatch?		
Notifications:		
Has the receiver been notified of the planned shipment, mode of transport, carriers, estimated time of arrival, name of driver (or drivers), and seal/lock identification numbers?		
Have relevant State and local governments been notified, including information on routes and estimated time of arrival?		
Acceptance of shipment:		
Is the Receiver prepared to: • Accept the shipment? • Verify the integrity and identification of the package(s) and conveyance? • Verify, during advance notification and in transport documents, that the carrier's and driver's identity are consistent with the information provided by the Shipper and consistent with direction from the Competent Authority? • Alert the Transport Security Manager, or its designee, of any discrepancies?		
Normal operations command and control		
Has an appropriate chain of command for the shipment been established and have all parties been made aware that, during operations associated with the transport of radioactive sources or radioactive material, the chain of command shall have full responsibility and authority for the shipment and any associated decisions relating to the shipment for both normal operations and emergency situations?		
Has a centralized command and control communications centre been established?		
Are centralized and continuous communications provided between: (1) the driver and accompanying personnel on the transport vehicle, (2) the driver and other escort personnel on each escort vehicle, and between all vehicles and a centralized command and control communications centre		
Is a GPS-based device, or other electronic-based tracking system, used that communicates position of the transport vehicle to the centralized command and control communications centre and to the escort vehicle?		
Do all operating personnel have a printed booklet of all relevant telephone numbers?		

	Security arrangements verification	Pre-shipment verification
Have the personnel in the transport vehicle and the personnel in its accompanying escort vehicle(s) been instructed to report to the specified centralized command and control communications centre at the departure of the shipment from the shipper site with an estimated time of arrival?		
Have the personnel in the transport vehicle or the escort vehicle been instructed that if there is any threat, emergency, delay in transit, unusual situation, or incident, it shall be immediately reported, as appropriate, to the centralized command and control communications centre?		
Have procedures been established and arrangements been made that dispatch of any needed additional security and/or emergency resources will be initiated and coordinated through the specified centralized command and control communications centre, and that it will also contact, as appropriate, State or local enforcement officials and coordinate information management controls?		
Have the command, communication, tracking, control and emergency response plans and procedures been appropriately developed and documented?		
Additional Security Measures		
Considering the threat or nature of the material being transported, including its attractiveness, should additional security measures be applied? (Specify reasons for considering additional security measures.)		
If additional security measures are to be applied, specify what they are and how they have been satisfied for this shipment		
Maintenance and Testing of Systems and Equipment		
Has an operability and functionality procedure for all equipment and communication devices to be used in the shipment been established?		
Has the operability and functionality of all equipment and communication devices to be used in the shipment been performed in accordance with the established operability and functionality procedure?		
What equipment and communication devices have been tested that applies to this security plan?		
Have procedures for testing and maintaining the transport vehicle been established?		
Has the maintenance and testing of the transport vehicle been performed in accordance with the established procedure?		
What equipment that applies to this security plan has been maintained and tested, and did the maintenance and testing satisfy all of the requirements established in the relevant maintenance and testing procedure?		
6. EMERGENCY RESPONSE		
Has an emergency response manual been developed that applies to this shipment (it may be a separate emergency response manual or part of a more comprehensive security manual)?		
Non-Tactical and Tactical Emergency Response		
Are local law enforcement organizations aware that they are to provide armed response in the event of an incident, including a security attack?		
Are the transport vehicle crew and the escort vehicle personnel aware that the procedures in the emergency response manual shall be followed in the event of an incident, including a security attack?		
In the event of any emergency or security threat, breach of security or other security incident, are the emergency response organizations aware that, if required, any needed medical action shall be taken in accordance with applicable procedures in the emergency response manual?		
In the event of any emergency or security threat, breach of security or other security incident, do both the crew of the transport vehicle and the escort vehicle car have in their possession the emergency response procedures defining the actions they should take?		
Has an arrangement been made and procedures been established with an applicable radiation protection agency to provide appropriate and timely radiological response in the event of a security attack or an incident?		

1

Incident Communications		
In the event of any emergency or security threat, breach of security or other security incident, has contact information for non-security related events been provided to involved personnel using the emergency response manual?		
Are the transport vehicle crew and/or the escort vehicle personnel aware that, in the event of an incident, including a security attack, they shall immediately contact the specified centralized command and control communications centre, providing detailed information regarding the attack?		
Has a centralized point of contact been arranged for establishing, with the State or local enforcement officials, appropriate and timely response in the event of a security attack or an incident?		
Upon notification by the transport vehicle crew and/or escort vehicle personnel of a security attack or an incident, is the specified centralized command and control communications centre aware that they shall immediately contact the relevant response force centralized point of contact defined in the transport security plan, and provide detailed information regarding the attack?		
Upon notification by the transport vehicle crew and/or escort vehicle personnel of a security attack or an incident, is the relevant response force centralized point of contact defined in the transport security plan aware that they shall contact, as needed, response forces (including military, if needed) to ensure adequate and timely mobilization of these forces?		
In the event of a security attack or an incident, is relevant centralized point of contact aware that they shall have overall responsibility for handling the tactical response at the scene of the attack in their bureau?		
In the event of a security attack or an incident, is the relevant involved radiation protection agency aware that they shall the responsibility for addressing radiological issues at the scene of the security attack or incident?		
Notification of Relevant Agencies		
Has the Receiver agreed to notify the Shipper if the consignment is not received as anticipated?		

1

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, Safety Requirements, 2012 Edition, IAEA Safety Standards Series No. SSR-6, IAEA, Vienna (2012).

[2] 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).

[3] 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, General Safety Requirements, Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

[4] UNITED NATIONS, Recommendations on the Transport of Dangerous Goods: Model Regulations, ST/SG/AC.10/1/Rev.18, UN, New York and Geneva (2013).

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

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

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

[8] European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), ,ECE/TRANS/242, UN, New York and Geneva (2015).

[9] Regulations concerning the International Carriage of Dangerous Goods by Rail (RID) (2015)

[10] European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterway (ADN), ECE/TRANS/231, UN, New York and Geneva (2015).

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

[12] 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).

[13] 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).

[14] FOOD AND AGRICULTURE ORGANIZATION, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE CO-ORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, Safety Requirements, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Preparing for Emergency Response to Transport Accidents Involving Radioactive Material, IAEA Safety Standards Series No. TS-G-1.2, IAEA, Vienna (2002).

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

[17] 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).

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

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004/Rev.1, IAEA, Vienna (2004).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on the Import and Export of Radioactive Sources, IAEA, Vienna (2012).[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime (NST020) under development

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Rev.5), IAEA Nuclear Security Series No. X, IAEA, Vienna (201X).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, Nuclear Security Series No. 8.

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, Nuclear Security Series No. 23-G.

[27] Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

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

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material, IAEA Safety Standards Series No. SSG-26, IAEA, Vienna (2012).