FOREWORD

[To be added later]
## CONTENTS

1. INTRODUCTION ........................................................................................................................................... 8
   1.1. Background............................................................................................................................................... 8
   1.1.1. Convention on the Physical Protection of Nuclear Material.......................................................... 8
   1.1.2. Recommendations and Guidance for Physical Protection of Nuclear Material in Transport 9
   1.1.3. Relationship to other International Documents................................................................. 9
   1.2. Objective............................................................................................................................................ 10
   1.3. Scope.............................................................................................................................................. 10
   1.4. Structure........................................................................................................................................ 11

2. OBJECTIVES OF THE STATE’S PHYSICAL PROTECTION REGIME FOR TRANSPORT OF NUCLEAR MATERIAL .......................................................................................................................... 13

3. ELEMENTS OF A STATE’S PHYSICAL PROTECTION REGIME FOR TRANSPORT OF NUCLEAR MATERIAL .......................................................................................................................... 14
   3.1. State Responsibility ...................................................................................................................... 14
       3.1.1. Fundamental Principle A – Responsibility of the State ......................................................... 14
       3.1.3. Establishing Transport Elements of a Physical Protection Regime ........................................ 14
   3.2. International Transport ............................................................................................................... 15
       3.2.1. Fundamental Principle B – Responsibilities during International Transport ...................... 15
       3.2.2. State Assignment of Responsibilities for the International Transport of Nuclear Material 15
   3.3. Assignment of Physical Protection Responsibilities..................................................................... 17
   3.4. Legislative and Regulatory Framework ..................................................................................... 18
       3.4.1. Fundamental Principle C – Legislative and Regulatory Framework ........................................ 18
       3.4.2. Fundamental Principle D – Competent Authority ................................................................. 19
       3.4.3. Fundamental Principle E – Responsibility of the Licence Holders ........................................ 21
   3.5. Identification and Assessment of Threats .................................................................................... 22
       3.5.1. Fundamental Principle G – Threat ....................................................................................... 22
       3.5.3. Review of Threat.................................................................................................................. 23
       3.5.4 Risk Informed Approach for Design of the Physical Protection System............................ 24
3.6  Fundamental Principle H – Graded Approach ................................................................. 24
3.7  Fundamental Principle I – Defence in Depth ................................................................. 25
3.8  Sustaining the Physical Protection Regime ................................................................. 26
3.8.1  Fundamental Principle F – Security Culture .......................................................... 26
3.8.2  Fundamental Principle J – Quality Assurance ....................................................... 27
3.8.3  Fundamental Principle L – Confidentiality ............................................................. 27
3.8.4  Sustainability Programme ...................................................................................... 28
3.9  Planning and preparedness for and Response to Nuclear Security Events ................. 29
3.9.1  Fundamental Principle K – Contingency Plans ....................................................... 29
3.9.2  Responsibilities of the State .................................................................................... 29
3.9.3  Responsibilities of the Shipper/Carrier .................................................................... 30
4.  CHARACTERIZATION OF NUCLEAR MATERIAL FOR APPLICATION OF TRANSPORT
    SECURITY ..................................................................................................................... 31
4.1  Nuclear Material Categorization Including Aggregation .............................................. 31
4.1.1  Nuclear Material Categorization ............................................................................. 31
4.1.2  Nuclear Material Aggregation ................................................................................. 33
4.2  Potential Additional Physical Protection measures for Category III and less than category III
    nuclear material ........................................................................................................ 36
4.3  Potential Radiological Consequences of Sabotage ....................................................... 38
4.4  Identification of Applicable Physical Protection Measures ......................................... 38
5.  DEVELOPMENT AND IMPLEMENTATION OF A TRANSPORT PHYSICAL PROTECTION
    REGIME - INCLUDING ROLES AND RESPONSIBILITIES OF THE SHIPPER, CARRIER AND
    RECEIVER .................................................................................................................. 40
5.1  Specifying and Applying Physical Protection .............................................................. 40
5.1.1  The prescriptive method ....................................................................................... 40
5.1.2  The performance-based method ............................................................................ 41
5.1.3  The combined method ......................................................................................... 41
5.1.4  Process for Applying the Methods ......................................................................... 42
5.2  General Responsibilities for Physical Protection in Transport ...................................... 43
5.2.1  Specific Responsibilities for Shipper ....................................................................... 44
5.2.2  Responsibilities for Shipper/Carrier ....................................................................... 44
5.2.3  Specific Responsibilities for Receiver ...................................................................... 44
5.3  Key Functions and Objectives of a Physical Protection System .................................... 44
5.3.1  Deter .................................................................................................................... 45
5.3.2  Detect ................................................................................................................... 45
5.3.3 Assess ............................................................................................................................ 45
5.3.4 Delay ............................................................................................................................. 45
5.3.5 Respond ......................................................................................................................... 45
5.4. Developing the Transport Security Plan ............................................................................... 46
5.4.1 Submitting and Obtaining Approval of the Transport Security Plan ......................... 47
5.4.2 Implementing the Transport Security Plan ................................................................... 48

6. MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN TRANSPORT ............................................................................................................................................. 50

6.1. Mode Independent Provisions ............................................................................................... 51
6.1.1 Common Requirements ................................................................................................. 51
6.1.2. Selection of Mode and Routing .................................................................................... 53
6.1.3 Assessment and Approval of the Transport Security Plan ............................................ 54
6.1.4. Authorization of Shipments .......................................................................................... 55
6.1.5. Advance Notification and Coordination ....................................................................... 56
6.1.6. Locks, Seals, Alarms and Engineered Systems ............................................................ 56
6.1.7. Written Instructions ....................................................................................................... 58
6.1.8. Inspections, Searches and Surveillance ......................................................................... 59
6.1.9. Communication and Confidentiality Involving the Shipper, Carriers and Receiver .... 60
6.1.10. Guards ........................................................................................................................... 61
6.1.11. Response Forces and Emergency Actions .................................................................. 62
6.1.12. Measures after Transport ............................................................................................ 63
6.1.13 Unplanned Stops ........................................................................................................... 63
6.1.14 Information Security ..................................................................................................... 64
6.2. Mode Specific Provisions ..................................................................................................... 64
6.2.1. Additional Provisions for Road Transport .................................................................... 64
6.2.2. Additional Provisions for Rail Transport ...................................................................... 67
6.2.3. Additional Provisions for Maritime Transport .............................................................. 67
6.2.4. Additional Provisions for Air Transport ....................................................................... 70
6.3. Additional Physical Protection Measures Based on Potential Radiological Consequences. 70

7. REQUIREMENTS FOR MEASURES TO LOCATE AND RECOVER NUCLEAR MATERIAL MISSING OR STOLEN DURING TRANSPORT ................................................................................................................................. 72
7.1. State Responsibilities ........................................................................................................ 72
7.2. The Carriers Responsibilities .......................................................................................... 73

8. MEASURES FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST SABOTAGE DURING TRANSPORT ................................................................................................................................. 75
8.1. General approach for designing measures against sabotage
8.1.1 Threat assessment and Design Basis Threat
8.1.2 Development of specific Threat scenarios
8.1.3 Target identification and ranking
8.1.4 Estimating the consequences of sabotage considering the threat and the targets: the Vulnerability Assessment
8.1.5 Results and conclusion of the vulnerability assessment
8.2. Defining Physical Protection Measures against Sabotage
8.2.1 Applicable Physical Protection Measures
8.2.2 Applicable Organizational Measures

9. MEASURES TO MITIGATE OR MINIMIZE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE DURING TRANSPORT
9.1. Responsibilities
9.2. Planning
9.3. Carrier Actions

REFERENCES

ANNEX I. THE TRANSPORT SECURITY PLAN

AI.1. Administrative Requirements/Information
AI.1.1. Allocation of Responsibilities
AI.1.2. Policies and Operational Procedures
AI.1.3. Training Requirements
AI.1.4. Information Management
AI.1.5. Trustworthiness of Personnel

AI.2. Shipment Security
AI.2.1. Description of the Nuclear Material to be Transported
AI.2.2. Description of the Security System
AI.2.3. Maintenance and Testing of Systems and Equipment
AI.2.4. Pre-Shipment Checks

AI.3. Response Planning
AI.3.1. Emergency Arrangements
AI.3.2. Contingency Plans
AI.3.3. Incident Communications, Command and Control

ANNEX II. THE VULNERABILITY ASSESSMENT
AI1. Planning the vulnerability assessment
1. INTRODUCTION

1.1. BACKGROUND

Threats to nuclear security involve criminals or terrorists acquiring and using for malicious purposes nuclear material to build nuclear explosive devices; and/or radioactive material to cause harm to individuals or the environment, including the construction of radiological dispersal devices (RDDs) and radiological exposure devices (REDs). Such threats could also include the dispersal of radioactive material through the sabotage of facilities in which radioactive material can be found or of such material in transport. These could be outsider/insider threats. The political and economic consequences, and the impact upon human health and the environment, of the malicious use of radioactive material could be severe, particularly in the case of a nuclear explosive device, and could be unpredictably disruptive in the case of malicious acts resulting in the dispersal of radioactive material.

1.1.1. Convention on the Physical Protection of Nuclear Material

The Convention on the Physical Protection of Nuclear Material (CPPNM) [1] for which the International Atomic Energy Agency (IAEA) is the depositary, provides the basis for the worldwide framework for ensuring the physical protection of nuclear material at nuclear facilities and during transport operations. The Convention obliges each State Party (i.e. each State that is a party to the Convention) to

1. meet defined standards of physical protection for both international shipments of nuclear material and domestic activities directly connected to such transport as set forth in the Convention,
2. cooperate in the recovery and protection of stolen nuclear material, and
3. define as criminal any acts to misuse nuclear material to harm the public. It is intended that each State Party, during international transport of Category I, II and III nuclear material, ensure the physical protection of the nuclear material within their territory or on board their ships in international waters or their aircraft in international airspace.

The Convention, however, does not oblige a State Party to meet defined physical protection standards for domestic transport of nuclear material that is not associated with international transport. To address this issue, and others, a Diplomatic Conference was convened in July 2005 to consider amendments to the Convention that had been proposed by 55 States that are parties to the Convention.

---

1 Historically, the term ‘physical protection’ has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities. As this publication is implementation guidance for Revision 5 of INFCIRC/225, the term physical protection is used throughout the publication.
As a result of this Conference, an Amendment to the Convention [2] was adopted that will also apply to each State Party as it ratifies the 2005 Amendment. The 2005 Amendment obliges each State Party to meet defined physical protection standards for domestic transport of nuclear material that is not associated with international transport.

Thus, for both domestic and international transport, multiple requirements apply to each State Party from the CPPNM. These include, but are not limited to requirements that each State Party:

- establish and implement a physical protection regime, which will include elements for the transport of nuclear material;
- consult and cooperate with other States Parties and other relevant organizations to design, maintain and improve its national system of physical protection and to properly design, maintain and improve its system of physical protection of nuclear material in international transport; and
- shall apply necessary steps to ensure that international transport of nuclear material under its jurisdiction is protected at appropriate levels.

1.1.2. Recommendations and Guidance for Physical Protection of Nuclear Material in Transport

To support the application of the CPPNM by a State, shippers, carriers and receivers, recommendations have been developed and issued as “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)” in Nuclear Security Series No. 13 (NSS-13) [3]. This publication sets out fundamental principles and recommended requirements to provide the essential elements of a State’s nuclear security regime (as defined in the Nuclear Security Fundamentals [4]) relating to the physical protection of nuclear material and nuclear facilities. Although NSS-13 provides recommendations on the physical protection of nuclear material in storage, use and transport it does not give technical guidance on implementation and compliance responsibilities for the transport of nuclear material. Therefore, it was felt desirable to provide an Implementing Guide to assist both State’s competent authorities and shippers/carriers operators in fulfilling their physical protection responsibilities in the transport of nuclear material.

1.1.3. Relationship to other International Documents

Although the CPPNM serves as the basis for promoting international cooperation for physical protection of nuclear material and nuclear facilities, it should also be recognized that other regulations, standards, codes, and guidelines developed for safety purposes may also apply, and can affect the development of the necessary security culture with all organizations involved in implementing physical protection, of a State’s physical protection regime, as well as the design and implementation
of a shipper’s/carrier’s physical protection system. Thus, such regulations, standards, codes, and
guides should be considered by a State for ensuring adequate levels of physical protection.

The IAEA has developed an Implementing Guide on “Security in the Transport of Radioactive
Material”, Nuclear Security Series No. 9 (NSS-9) [5], which establishes “security levels for the
protection of radioactive materials during transport and appropriate physical protection measures
commensurate with the potential radiological consequences that could result from malicious use of
radioactive material”. The radioactive material security in transport guidance publication applies “to
the transport of all packages containing radioactive material — including nuclear material … — that
may pose a significant radiological hazard to individuals, society and the environment if the material
is used in a malicious way” and therefore it addresses only the concerns regarding potential
radiological consequences should nuclear material be used in a radiological dispersion device. It does
not address concerns regarding the use of nuclear material in an nuclear explosive device or the
potential consequences of sabotage. Thus, the guidance provided for security in the transport of
radioactive material is complementary to, but not sufficient for, the physical protection needed for the
transport of nuclear material Category I, II and III nuclear material.

Application of the guidance provided in this publication will allow for physical protection of nuclear
materials to work in concert with and not conflict against the controls for safety during the packaging
and transport of all radioactive material established through the Regulations for the Safe Transport of
Radioactive Material (‘the Transport Regulations’) [6] and with other safety and security publications
produced at the international level.

1.2. OBJECTIVE

The objective of this publication is to provide guidance to States and their competent authority or
authorities on how to implement and maintain a physical protection regime for transport of nuclear
material. This publication may also be useful to shippers and carriers in the design and implantation of
their physical protection systems. This publication builds upon the recommendations outlined in NSS-
13 and provides additional guidance on how to implement these recommendations into practice.
Consistent with NSS-13, the guidance provided in this publication is for consideration by States and
their competent authorities but are not mandatory upon a State and do not infringe on the States
sovereign rights.

1.3. SCOPE

This publication applies to physical protection of nuclear material in transport. It provides guidance
for protection against three types of malicious acts;
— unauthorized removal with the intent to construct a nuclear explosive device,
unauthorized removal which could lead to subsequent dispersal,
sabotage.

This publication explores and elaborates upon the requirements and recommendations described in the CPPNM and NSS-13 to provide detailed guidance on the implementation of physical protection in transport.

It is achieved by:

explaining how the fundamental principles described in NSS-13 apply to transport,
providing guidance to States and their competent authorities on how to categorize nuclear material for the application of physical protection measures (including aggregation),
providing additional guidance to States and their competent authority, shippers and carriers on how to protect against those acts described above.

This publication also includes actions undertaken to locate and recover nuclear material immediately after recognizing the material is missing, prior to the reporting of lost, missing or stolen nuclear material. Detailed information about this can be found in “Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control”, Nuclear Security Series No. 15 (NSS-15) [7].

This publication is intended to provide guidance for security in transport of nuclear material in the public domain. However, the recommendations may be applied to on-site transports as the State deems necessary.

1.4. STRUCTURE

This publication is structured following the structure of NSS-13. The structure is as follows:

Section 2 summarizes the objectives arising from NSS-13 that relate to a State developing the transport elements of a State’s physical protection regime;
Section 3 presents a discussion of the responsibilities of the State in establishing and maintaining a physical protection regime that includes those elements necessary for ensuring physical protection of nuclear material in transport;
Section 4 elaborates on the categorization of nuclear material for application of transport security;
Section 5 elaborates on the responsibilities of the shipper and carrier in developing and implementing physical protection system for specific shipments of nuclear material; establishing, implementing and maintaining a physical protection system for those shipments with emphasis on the development and application of Transport Security Plans;
— Section 6 elaborates on measures to be taken to protect against unauthorized removal of nuclear material in transport by listing specific baseline guidance for the application of the prescriptive method of developing a physical protection system that is expected to provide adequate physical security transport. This baseline guidance follows a graded approach according to the classification of the nuclear material, providing mode independent, mode specific, and international provisions;

— Section 7 elaborates on measures to be taken to locate and recover nuclear material missing or stolen during transport;

— Section 8 discusses measures for physical protection of nuclear material against sabotage in transport;

— Section 9 discusses measures to mitigate or minimize the radiological consequences of sabotage in transport; and

— Annex I provides a listing of sample contents for a Transport Security Plan

— Annex II provides a summary of a Vulnerability Assessment

— Definitions of terms used in this Implementing Guide are listed at the end of the publication.
2. OBJECTIVES OF THE STATE’S PHYSICAL PROTECTION REGIME FOR TRANSPORT OF NUCLEAR MATERIAL

NSS-13 [3] states that: “The overall objective of a State’s nuclear security regime is to protect persons, property, society, and the environment from malicious acts involving nuclear material and other radioactive material. The objectives of the State’s physical protection regime, which is an essential component of the State’s nuclear security regime, should be:

— **To protect against unauthorized removal.** Protecting against theft and other unlawful taking of nuclear material.

— **To locate and recover missing nuclear material.** Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material.

— **To protect against sabotage.** Protecting nuclear material and nuclear facilities against sabotage.

— **To mitigate or minimize effects of sabotage.** Mitigating or minimizing the radiological consequences of sabotage.”

“The State’s physical protection regime should seek to achieve these objectives through:

— Prevention of a malicious act by means of deterrence and by protection of sensitive information;

— Management of an attempted malicious act or a malicious act by an integrated system of detection, delay, and response;

— Mitigation of the consequences of a malicious act.”

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

Each of these objectives applies to transport security. This Implementing Guide addresses actions which can be taken towards meeting these objectives in transport.
3. ELEMENTS OF A STATE’S PHYSICAL PROTECTION REGIME FOR TRANSPORT OF
NUCLEAR MATERIAL

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

This section:

— lists each Fundamental Principle and other key elements of the State’s physical protection
   regime, as presented in NSS-13,
— considers the implementation of each principle as applied to transport activities.

3.1. STATE RESPONSIBILITY

3.1.1. Fundamental Principle A – Responsibility of the State

Responsibility of the State – The responsibility for the establishment, implementation and
maintenance of a physical protection regime within a State rests entirely with that State.

It is incumbent upon a State to take appropriate steps to provide a framework that will ensure a sound
nuclear material physical protection regime exists within its State, including those elements of the
regime relating to physical protection of nuclear materials in transport. (NSS-13, 3.1)

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

3.1.3. Establishing Transport Elements of a Physical Protection Regime

The State should ensure that a comprehensive physical protection regime for transport of nuclear
material is established, implemented and maintained. This physical protection regime includes: (a)
the legislative and regulatory framework governing the physical protection of the nuclear material in
transport; (b) the institutions and organizations within the State responsible for ensuring the
implementation of the legislative and regulatory framework, and; (c) the transport-specific physical
protection systems. Within this context, physical protection in transport should be an integral part of
the State's overall physical protection regime for nuclear material. (NSS-13, 3.1)
A State should accomplish its responsibilities by having an adequate and supportive legislative base and governmental organization. This should include the State designating a competent authority or competent authorities that are responsible for enforcing the State’s requirements.

The physical protection elements of the State's nuclear security regime relating to nuclear material transport should also be reviewed and updated regularly by the competent authority or competent authorities to reflect changes in the threat and advances made in physical protection approaches and technologies. (NSS-13, 3.2)

The State should ensure that the competent authority has effective independence. This means that organizational units that are responsible for licensing and supervisory activities are protected by regulatory or organizational means against any undue influence by other units or bodies on the execution of their tasks. If the transport elements of the State’s regime of physical protection are divided between two or more authorities, arrangements should be made for overall co-ordination. Clear lines of responsibility should be established by every State assigned and recorded between the relevant entities so that continuous protection of the material is ensured.

3.2. INTERNATIONAL TRANSPORT

3.2.1. Fundamental Principle B – Responsibilities during International Transport

Responsibilities during International Transport – The responsibility of a State for ensuring that nuclear material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate.

A State’s physical protection regime should ensure adequate physical protection of nuclear 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. (NSS-13, 3.3)

3.2.2. State Assignment of Responsibilities for the International Transport of Nuclear Material

Responsibility for establishing and implementing a comprehensive physical protection regime within a State rests entirely with the State. When international transport is involved there is also need for effective international cooperation, including liaison with involved international bodies and organizations, until responsibility is transferred to another State. Only by assuring continuity of security responsibilities during the entire transport operation can a State fulfil this principle. (NSS-13, 3.3)

The State has responsibility for physical protection of nuclear material within its borders and on aircraft and ships registered under its flag when they are carrying nuclear material in international
airspace or waters, until responsibility is transferred to another State. States involved in international transport should ensure that coordination with transit or receiving States is undertaken so that continuous and adequate protection of the material is ensured as responsibility for the nuclear material is transferred from one State to another. (NSS-13, 3.4)

International shipments may involve land transport by road or rail, modal transfers, transport by aircraft or ships, transit through multiple States and in-transit storage. In all cases the relevant competent authority should make sure that the security of the material is assured throughout the shipment and that the point of transfer of responsibilities to another State is clearly defined. For land transports, the point of transfer of responsibilities to another State will be dictated by the States concerned. Owing to the nature of maritime shipments and the jurisdiction of the flag of registration of the transport vessel (flag State) concerned, the point of transfer of responsibility should be clearly defined until material is properly transferred to / from the receiving State. In cases where a ship with nuclear material is transiting through other States’ territorial waters, the responsibilities for security should be clearly defined until the ship resumes passage in international waters. For air transports, notwithstanding the flag State of the aircraft, the point of transfer of responsibility will normally be the point at which the material is loaded/discharged, under agreement between the States.

The shipping State should ensure that all involved States are prepared to accept these responsibilities before a shipment is authorized. NSS-13 provides several ways in which a State can ensure that involved States, including transit States are prepared to accept these responsibilities:

- verifying that all States are Parties to the CPPNM; or
- concluding formal agreements to ensure physical protection will be implemented in accordance with international agreements; or
- obtaining formal declarations that physical protection will be provided in accordance with internationally accepted guidelines; or
- ensuring that licences or authorizations containing appropriate physical protection arrangements have been issued. (NSS-13, 3.5 and 3.7)

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

In addition, when international shipments of nuclear material transit the territory of States other than the shipping State and the receiving State, the arrangements between the shipping and receiving States should identify the other States that are involved in such a transit with a view to informing them and obtaining, in advance, their cooperation and assistance for adequate physical protection measures and for recovery actions in the territory of such States in case of loss of, attack on, or sabotage of an
international shipment. It should be noted that the proposed arrangements, resulting from advance notifications among States involved, do not affect the exercise of navigation rights and freedoms by ships and aircraft as provided for in International law. (NSS-13, 3.6 and 3.7, and footnote 3 for para. 3.6 in NSS-13)

Consistent with the graded approach, in the case of international shipments of Category III nuclear material transiting international waters or air space, it will generally be sufficient for shippers/carriers to ensure that physical protection arrangements in other States jurisdictions are in accordance with those State’s requirements. International shipments of Category III are normally shipped by normal commercial transport shipping companies. The shipping State should determine if the transit or receiving States have notification or other requirements applicable to that transit or receipt of Category III material.

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

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

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

Arrangements for the shipment, including the points at which responsibility is transferred from one State to another should be concluded sufficiently in advance so that all affected States can complete their physical protection arrangements. (NSS-13, 3.7)

In the case where agreements and arrangements involve the exchange of sensitive information, arrangements must be made to accomplish this while protecting the information appropriately; this may involve shipping, receiving and transit States.

3.3. ASSIGNMENT OF PHYSICAL PROTECTION RESPONSIBILITIES

A State’s physical protection regime should include an integrated assignment of physical protection responsibilities at all levels of government, including response forces.
The State should ensure that physical protection responsibilities during transport are clearly assigned to the shipper, the carrier, the receiver or other relevant entity. Where the term “shipper/carrier” is used in the rest of the publication, it refers to the entity to which any specific physical protection responsibility related to transport is assigned. Specific physical protection responsibilities may also be assigned specifically to the shipper, the receiver, etc.

States can hold the operator responsible for physical protection during transport and this will require that the operator either conduct the transport operation themselves or use a carrier which implements physical protection measures under the direction of the operator.

Alternatively, the State can assign the physical protection responsibilities to authorized carriers and the operator/shipper can then rely on the carrier's physical protection system. (NSS-13, 3.8)

The State's physical protection regime should also establish and assign clear lines of responsibility for response to all nuclear security events during transport. These responsibilities may include multiple levels of government and should, as appropriate to the Category of material concerned, clearly indicate responsibilities for response, including those of the shipper and/or carrier during transport. (NSS-13, 3.8)

3.4. LEGISLATIVE AND REGULATORY FRAMEWORK

3.4.1 Fundamental Principle C – Legislative and Regulatory Framework

**Legislative and Regulatory Framework** – The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of nuclear facilities and transport to verify compliance with applicable requirements and conditions of the licence or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions.

The State should ensure that a comprehensive legislative and regulatory framework is established with the jurisdiction and responsibility to ensure the physical protection of shipments of nuclear material. The legislative and regulatory framework for physical protection in transport should be an integral part of the State's overall physical protection regime. (NSS-13, 3.9)

The legislative and regulatory framework for the transport of nuclear material should include the designation, funding and staffing of a transport security competent authority, with authority and

---

2 In many States this entity is the licence holder.
responsibility for ensuring that the State’s requirements for physical protection in transport are understood and adhered to by shippers/carriers under the State’s jurisdiction.

Enforcement of physical protection regulations is a necessary part of a State's physical protection regime. Thus, for transport of nuclear material, the State should assign the power to initiate legal proceedings or to impose sanctions in accordance with the law, where such sanctions may involve suspension of licence, and/or penalties. (NSS-13, 3.15)

### 3.4.2. Fundamental Principle D – Competent Authority

**Competent Authority** – The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State’s competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.

The legislative and regulatory framework for the transport of nuclear material should include the designation, funding and staffing of the competent authority, whose functions should include:

- licensing or authorizing shippers or carriers to transport nuclear material; performing inspections of nuclear material transports to ensure shipments are undertaken in full compliance with the applicable requirements and conditions established by the competent authority,
- defining requirements or objectives for physical protection in transport based on the threat assessment or design basis threat. These requirements or objectives should take into account both physical protection against unauthorized removal of nuclear material and potential consequences of sabotage. The competent authority should ensure that the more stringent requirements or objectives are applied,
- specifying requirements for Transport Security Plans (TSPs),
- promulgating comprehensive regulations for physical protection in transport. These regulations should be periodically reviewed for adequacy,
- performing evaluations, consistent with a graded approach and including exercises where appropriate, to test the transport physical protection systems, training and readiness of guards and/or response forces,
- ensuring trustworthiness determinations, using a graded approach, for all personnel that have physical protection responsibilities during transport or access to sensitive information,
- establishing a means to enforce applicable requirements and conditions (NSS-13, 3.10 to 3.14),
— defining what transport related information should be considered as sensitive and ensuring that its confidentiality is protected accordingly.

The State’s competent authority should have a clearly defined legal status, independence from operators, shippers and carriers and have the legal authority and capabilities to perform its responsibilities and functions effectively. (NSS-13, 3.18)

3.4.2.1 Competent Authority Role in Requiring Transport Security Plans for Nuclear Material

The competent authority needs to effectively communicate to shippers those requirements that they must satisfy in order to design and implement a physical protection system that will be acceptable under the State’s physical protection regime. An important element of this regime will be the design of and compliance with a TSP, appropriate to the Category of material being transported. The competent authority should issue instructions to shippers concerning requirements for a TSP which should ensure that all elements of a State’s physical protection requirements are met.

The competent authority should ensure there is clear responsibility for, and ownership of, the TSP. For Category I and II nuclear material, the TSP should address routing of the shipment, stopping places, destination hand over arrangements, identification of persons authorized to take delivery, emergency arrangements, contingency plans and reporting procedures (routine, non-compliance and emergency). The competent authority also may require that less sensitive nuclear material transports are subject to a similar, or modified, process dependent on the State’s requirements or assessment of the threat; e.g. the competent authority may require that less sensitive transports are conducted in accordance with plans which may be generic and which reflect previously approved standards and measures.

Information required in a TSP under these provisions may be incorporated into plans developed for other purposes. However, TSPs will, invariably, contain information that should be restricted to those who need to know it for the performance of their duties. Such information should not be included in plans developed for other purposes and that may be disseminated more widely.

3.4.2.2 Role of Competent Authorities in Establishing an Inspection Regime

The State’s competent authority is responsible for verifying continued compliance with transport physical protection regulations and applicable licence conditions through regular inspections and for ensuring that corrective actions are taken, when needed.

The objective of an inspection regime is to verify the compliance of measures actually in place against regulatory requirements and applicable licence conditions; this may be accomplished by inspection to verify compliance with the TSP.
Inspections should be performed by qualified and suitably trained State personnel or designees and may include both announced and unannounced inspections. The State may specify requirements to the inspectors such as qualification or training. Inspections should take place during transport operations and at shippers/carriers main offices or premises. This will ensure that all physical protection measures, including technical, procedural, and administrative provisions are reviewed and evaluated. Inspections conducted during transport operations, on departure, on arrival, and during rest stops, etc. should not impede or unduly affect the normal progress of the shipment.

In the event that inspections discover malfunctions, non-compliance or any other issues, the consequences of these findings should be graded and acted upon commensurately. Inspectors should define with shipper/carrier on deadlines to complete corrective actions, monitor progress and follow up actions to ensure they have been completed to an acceptable standard.

The number of inspections conducted should be determined by the number of shipments the shipper or carrier have completed, how compliant they are, the threat assessment and any other relevant factors. However, all carriers/shippers should be inspected at least annually or on any other suitable periodic basis to ensure continued compliance.

3.4.3. Fundamental Principle E – Responsibility of the Licence Holders

Responsibility of the Licence Holders – The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licences or of other authorizing documents (e.g., operators or shippers).

The State should ensure that shippers/carriers are assigned the primary responsibility for implementing a sound physical protection system for the transport of nuclear materials. In fulfilling these responsibilities, the shippers should comply fully with the regulations and other requirements issued by the competent authority. (NSS-13, 3.24)

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

If deficiencies are discovered in the transport physical protection system that prevent it from providing the required level of protection, the shipper and/or carrier are responsible for taking immediate compensatory measures to ensure appropriate protection for the shipment. These measures should be closely coordinated between the shipper and carrier, and when necessary, with other involved entities such as the competent authority and response forces. The shipper and/or carrier should then implement corrective action and have these actions approved by the competent authority.

3.5. IDENTIFICATION AND ASSESSMENT OF THREATS

3.5.1 Fundamental Principle G – Threat

Threat – The State’s physical protection should be based on the State’s current evaluation of the threat.

The State should assess the known and postulated threats, related to nuclear material transport and ensure that the evaluation is adequate and maintained current. The State’s threat assessment should consider all pertinent factors including the nature, quantity and relative attractiveness of the nuclear material transported, and the potential radiological and other consequences that could result from any unauthorized act directed against the nuclear material in transport, including sabotage. The State may communicate the results of the threat assessment to the shipper/carrier as a guide in the development of its TSP. Alternatively, the State can base its regulatory framework on its evaluation of the threat and require physical protection measures appropriate to counter the threat. The State may wish issue a Design Basis Threat (DBT) for transport.


Fundamental Principle G specifies that the State should base its physical protection regime on a current evaluation of the threat. States will vary in their ability to identify and evaluate threat. Some States have sophisticated security and intelligence capabilities that can assist the competent authority in understanding the nature and extent of threats, including those that might be directed toward nuclear material transport. In other cases, general information about the national threat (civil unrest, criminal activities, terrorist presence, etc.) will need to be understood and evaluated to identify the potential threat within a country. In all cases this should be done cooperatively among the State agencies that have responsibilities for understanding and responding to threat (intelligence, police,
A military etc.). Based on this evaluation of the threat, the competent authority can make decisions on how to effectively counter the threat with physical protection in transport. (NSS-13, 3.34 and 3.35)

Three distinct methods for specifying requirements to address the assessed threat are defined in Section 5.5. These three methods are (a) the prescriptive method, (b) the performance-based method, and (c) the combined method. For each category of nuclear material shipped, whichever method is followed, the physical protection measures applied should either comply with the administrative and technical requirements specified in the State’s regulatory framework (for the prescriptive method and some options of the combined method), or should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment (for the performance-based method and other options of the combined method).

Following a graded approach methodology the competent authority may choose to (a) apply one of these methods to all three categories of nuclear material, (b) specify different methods be used for different categories of material, or (c) allow more than one method to be used for a given category of material. For example, the State may choose to specify that the prescriptive method be used for all nuclear material shipments. In this case the State should assure itself that the prescribed physical protection measures are sufficient to counter the assessed threat or DBT. Alternatively, the State may choose to specify that (a) the prescriptive method be used for shipments of Category III nuclear material; (b) either the prescriptive or the combined method be used for shipments of Category II nuclear material, and (c) only the performance-based method be used for shipments of Category I nuclear material.

3.5.3. Review of Threat

The State should continuously review the threat and evaluate the implications any change to the threat assessment may produce. The State’s competent authority should take steps to ensure that any change is appropriately reflected in their regulatory framework and in the shipper’s or carrier’s physical protection measures. Recognizing that a revision of the DBT may take additional time in this process, short term compensatory physical protection measures based on the current threat assessment should be implemented. The effectiveness of these measures against the current threat should be evaluated. The DBT should then be reviewed in the light of the revised threat assessment (NSS-13, 3.39).

In the event of a change in threat, particularly one indicating a direct threat towards nuclear material transports, a State’s competent authority should consider directing a shipper/carrier to postpone or cancel a movement.
3.5.4 Risk Informed\(^3\) Approach for Design of the Physical Protection System

3.5.4.1 Risk management

The State should use a risk management approach to ensure that its physical protection regime is keeping the risk of unauthorized removal or sabotage during transport at an acceptable level. This consists of evaluating the threat and potential consequences of such acts and ensuring that appropriate physical protection measures are put into place to prevent or minimize the likelihood of a successful malicious act. (NSS-13, 3.41)

Risk management takes into account an assessment of risk which can be quantitative or qualitative. Quantitative risk assessment involves determining the probability of an event occurring and multiplying it by the potential consequences of the event. The probability of a malicious act occurring or being attempted is very difficult to quantify and therefore in some cases is assumed to be one. Qualitative risk management 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. (NSS-13, 3.41)

The results of the risk analysis identify areas where vulnerabilities should be identified and further evaluated to determine if additional measures should be required to reduce the security risk. Risk can be reduced through, for example, deterrence (appearance of robust physical protection measures), strengthening physical protection measures (e.g. additional defence in depth, increasing the conveyance/package resistance to attack, strengthened information security, etc.) and reducing potential consequences (e.g. the chemical or physical form of the material being transported). (NSS-13, 3.42)

3.6 FUNDAMENTAL PRINCIPLE H – GRADED APPROACH

**Graded Approach** – Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities.

The development of the State’s physical security regime should be structured around a graded approach which is used to provide higher levels of protection against events that could result in higher

\(^3\) Within the context of this publication, the term risk-informed approach is used to harmonize with the IAEA nuclear security fundamentals. The term “risk based” is used in NSS-13.
consequences. In doing this, the State should consider what level of risk is acceptable and what level of protection against the threat should be provided. (NSS-13, 3.43)

For protection against unauthorized removal for use in an nuclear explosive device, the category of the nuclear material, as defined in NSS-13, Table 1, reflects the relative difficulty of producing consequences from construction of a nuclear explosive device. Therefore in accordance with the Graded Approach, Category I material must be protected with the most stringent levels of physical protection, whereas materials below Category III need only be protected with prudent management practices (as defined in NSS-9) and (NSS-13, 3.44).

For protection against sabotage and unauthorized removal for subsequent dispersal, the State needs to consider the potential radiological consequences of such acts and provide graded protection measures on this basis. The State should consider how to protect material taking account its potential to cause an unacceptable radiological consequence and ensure that protection measures are required for material capable of producing such consequences. Nuclear material with potential radiological consequences should be protected with physical protection measures that are commensurate with those potential consequences. IAEA Nuclear Security Series No. 9, Security in the Transport of Radioactive Material (NSS-9), provides guidance on this. (NSS-13, 3.44)

In addition to the principle of using the concept of the graded approach for physical protection measures, a State should consider the use of this concept to define the levels of other physical protection measures, such as confidentiality (Section 3.7.2) and trustworthiness of individuals.

3.7. FUNDAMENTAL PRINCIPLE I – DEFENCE IN DEPTH

Defence in Depth – The State’s requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives.

The State should incorporate the concept of defence in depth in the measures that it requires for protection of nuclear material in transport. Because transport often takes place in the public domain and in a less controlled environment than at a fixed facility, defence in depth should be used by the State in establishing and specifying its requirements for physical protection in transport. (NSS-13, 3.45)

The State requirements should reflect the concept of several layers and methods of protection that have to be overcome or circumvented by an adversary. More specifically, State requirements for physical protection should be based on the concept of defence in depth for preventive and protective measures. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their
duties) and the design of the transport equipment (conveyance, any protective overpacks, package, etc.). Therefore, the shipper or carrier’s physical protection system should be designed specifically for each shipment, or equivalent set of shipments, taking into account the State’s defined threat or DBT. (NSS-13, 3.45)

The State should require that the defence in depth approach is incorporated in the design of the physical protection system for the functions of detection, delay and response. Each function should 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. Delay can consist of multiple independent physical barriers such as the conveyance enclosure, protective overpacks, the package and securing these so the adversary task time is increased.

3.8. SUSTAINING THE PHYSICAL PROTECTION REGIME

3.8.1 Fundamental Principal F – 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.

Nuclear security culture plays an important role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to prevent and combat the threat of sabotage or using nuclear material for malicious acts. A nuclear security regime includes a range of elements and activities, including: legislation and regulation; intelligence gathering; assessment of the threat to nuclear material and associated locations and facilities; administrative systems; various technical hardware systems; response capabilities and mitigation activities. No single government or industry organization or subsection of such an organization can address these elements in isolation. An effective nuclear security culture is dependent on proper planning, education, training, awareness, operation and maintenance, as well as on people who plan, operate and maintain nuclear security systems. Even a well-designed system can be degraded if the procedures necessary to operate and maintain it are poor, or if the shipper/carrier fails to follow procedures. Ultimately, therefore, the entire nuclear security regime stands or falls because of the people involved and their leaders, and it is the human factor, including management leadership, that must be addressed in any effort to enhance the existing nuclear security culture. Nuclear security culture might in some cases help at countering the insider threat

As transport occurs in the public domain, it is important that all involved in transport operations are aware of the need to establish and maintain a strong security culture. It should also be remembered
that some States may choose to licence carriers of nuclear material rather than rely on a shipper’s contractual conditions and the competent authority should consider how to address and promote a security culture among personnel who may have no nuclear background. This could be achieved by regular briefings on the threats posed by a poor security culture in order to raise awareness of all involved as well as imposing licence conditions designed to enhance the overall company security policy.

In transport operations a strong safety culture is also extremely important. A strong safety culture includes elements of openness and transparency with regard to information. Thus, a balance needs to be maintained with respect to concepts of confidentiality of sensitive information, which is an important element of security culture.

### 3.8.2 Fundamental Principle J – Quality Assurance

**Quality Assurance** – A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.

The State should, within its regulatory framework, require that a shipper or carrier establish and implement a quality assurance policy and programme to ensure that where a physical protection system is designed, implemented, operated or maintained, it is done so to a standard capable of effectively responding to the threat assessment or DBT and that meets the State’s regulations. This will ensure, as far as practicable, that all physical protection measures associated with the transport of nuclear materials are performed at an acceptable level. (NSS-13, 3.52)

A quality assurance program should encompass all security related activities (technical, procedural and administrative) and be reviewed on a periodic basis. For Category I transports, shipper’s or carrier’s should ensure that all relevant physical protection measures (tracking system, communications equipment, sterile areas etc.) are operating correctly, this should then be confirmed to the State’s competent authority before the transport commences.

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

### 3.8.3 Fundamental Principle L – Confidentiality

**Confidentiality** – The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities.
Each State should establish requirements for protecting the confidentiality of sensitive information relating to the transport of nuclear materials. Such information may include the design and operation of the transport physical protection system and the specifics of a shipment (timing, route, contingency plans etc.). The unpredictability of shipments is vital in limiting the time and opportunities that an adversary will have to undertake a malicious act. (NSS-13, 3.53)

The State should take steps, consistent with national requirements and procedures, to ensure appropriate protection of specific or detailed information relating to transport operations, the unauthorized disclosure of which could compromise the physical protection of nuclear material. This includes identifying what information needs to be protected and the level at which it must be protected, using a graded approach (Section 3.6.2). It should define in its regulatory framework the provisions that a shipper should follow for ensuring the confidentiality of information and documentation relating to physical protection systems. Management of physical protection systems should limit access to sensitive information to those who have a need to know for the performance of their duties. Information addressing possible vulnerabilities in physical protection systems should be highly protected. (NSS-13, 3.53 and 3.54)

The State should be mindful that on occasion, particularly for Category III transports, that information may need to be passed to a range of recipients for operational purposes (ferry bookings, transport network requirements etc.) and that protection of this information is suitably proportionate yet not so stringent that it may impact transport operations.

Sanctions are a necessary component relating to confidentiality. Sanctions against persons violating confidentiality should be part of the State’s legislative or regulatory system, and should be severe enough to act as a deterrent against such actions. States should make such offences punishable by appropriate penalties which take into account their potentially grave nature. (NSS-13, 3.55)

3.8.4. Sustainability Programme

Sustaining the effectiveness of the State’s physical protection is necessary to ensure it remains effective in the long term. The State should establish a sustainability program to ensure that the necessary resources are committed to this effort, including by shippers and carriers. (NSS-13, 3.56 and 3.57)

Shippers and carriers should have sustainability programs for their physical protection systems that encompass:

- operating procedures and instructions to personnel (specific to role)
- human resources management and training
- equipment – maintaining, updating, repair and calibration
— performance testing and monitoring of operating systems
— configuration management – ensuring the physical protection system (including computer
system) is configured as designed and that any changes are properly designed, verified and
implemented
— resource allocation to ensure continued performance of the physical protection system

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

3.9.1. Fundamental Principle K – Contingency Plans

Contingency Plans – Contingency (emergency) plans to respond to unauthorized removal of nuclear
material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared
and appropriately exercised by all licence holders and authorities concerned.

In the event that a malicious act occurs against a shipment of nuclear material, the State, the
shipper/carrier and all others involved in the shipment should be properly trained and prepared to
respond. This should be accomplished by having adequate contingency planning, which should
include periodically testing and exercising the plans prior to undertaking shipments.

The development of contingency plans, and incorporation of these plans into the overall plans for
response to any emergency, should be a joint effort between the State and the shippers/carriers. Thus,
the State’s regulatory framework should clearly specify the requirements for emergency planning;
what emergency response capabilities are to be provided by the State, what are to be provided by the
private sector, and how these are to be coordinated.

The goal of emergency planning and response is to ensure a timely and effective response at all levels
in the event of an emergency involving the transport of nuclear material, whether it is an attack, an
accident, a medical emergency or a natural disaster involving the transport operation. It is essential
that the correct actions and decisions are taken at the right time to adequately respond and resolve the
situation. Arrangements should be made to ensure the continued effectiveness of the physical
protection system during any emergency. This requires careful and integrated planning by the State,
shipper and carrier. (NSS-13, 3.61)

3.9.2. Responsibilities of the State

The State should establish a security contingency plan to respond to emergencies involving nuclear
material transports. This should consist of actions to be taken in the event of theft, sabotage and
serious accidents involving nuclear materials in transport that are considered beyond shipper/carrier
control or capability. These plans should cover transports of nuclear materials both domestically and
Internationally. In addition, the contingency plans should be harmonized with the national response plan for nuclear security events [NSS-15].

3.9.3. **Responsibilities of the Shipper/Carrier**

In accordance with the State’s regulatory framework, a shipper/carrier should establish, implement and exercise security contingency plans for nuclear material transports. These plans should cover responses to all conceivable scenarios, malicious or other (theft, sabotage, illness, accident, breakdown etc.), and be approved by the State’s competent authority.

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

Coordination between guards that may be accompanying shipments and response forces should be regularly exercised. Transport personnel should be trained and prepared to act in full coordination with the guards, response forces and other response teams in accordance with the contingency plan. (NSS-13, 3.60)

Whenever there is detection and assessment of a malicious act the shipper/carrier should immediately initiate its contingency plan (NSS-13, 3.62)
4. CHARACTERIZATION OF NUCLEAR MATERIAL FOR APPLICATION OF
TRANSPORT SECURITY

Nuclear material should be evaluated in two ways in order to determine appropriate physical
protection requirements to prevent unauthorized removal during transport:

— for use in construction of a nuclear explosive device
— based on potential radiological consequences if dispersed or used for other malicious
  purposes.

Additionally, the potential radiological consequences of sabotage should be taken into account and for
those instances where protection against sabotage warrants additional protective measures, they
should be applied as well. (NSS-13, 6.3)

This approach accounts for all three ways the nuclear material might be used in a malicious act
(nuclear explosive device, radiological dispersal device and dispersal as a result of sabotage). Each of
these three considerations is addressed in more detail in the following Sections. Based on
consideration of all three types of potential malicious acts involving nuclear material the appropriate
(i.e., most stringent) physical protection measures can be identified and applied.

4.1. NUCLEAR MATERIAL CATEGORIZATION INCLUDING AGGREGATION

4.1.1 Nuclear Material Categorization

The primary factor in determining the physical protection measures for unauthorized removal of
nuclear material is the potential for the material to be used in a nuclear explosive device. Table 1 of
NSS-13 (reproduced in this Section) categorizes nuclear material on the basis of the element, isotope,
quantity of material and irradiation (if any). This categorization provides a basis for specifying
appropriate physical protection measures against unauthorized removal. There are other aspects of
nuclear material that render such material more or less attractive to an adversary, including physical
and chemical form, and degree of dilution. (NSS-13, 4.5 and 6.4) By detailing the categories in Table
1 (e.g. sub-categorize) or assigning particular material, the State may define specific physical
protection measures to that category or material.

While footnote "e" of Table 1 provides the option of reducing the nuclear material category for
irradiated fuel by one category, States should carefully consider whether or not to do this since it is
based on the premise that the radiation levels are sufficient to incapacitate an adversary before they
can complete the malicious act. There are many plausible scenarios where an adversary with basic
knowledge and resources can complete the malicious act before incapacitation due to radiation dose.
States may establish subcategories in order to specify physical protection measures for the subcategories for particular materials (NSS-13, 4.6).

**TABLE 1: CATEGORIZATION OF NUCLEAR MATERIAL**

<table>
<thead>
<tr>
<th>Material</th>
<th>Form</th>
<th>Category I</th>
<th>Category II</th>
<th>Category III</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Plutonium*</td>
<td>Unirradiated†</td>
<td>2 kg or more</td>
<td>Less than 2 kg but more than 500 g</td>
<td>500 g or less but more than 15 g</td>
</tr>
<tr>
<td>2. Uranium-235</td>
<td>Unirradiated†</td>
<td>5 kg or more</td>
<td>Less than 5 kg but more than 1 kg</td>
<td>1 kg or less but more than 15 g</td>
</tr>
<tr>
<td></td>
<td>- uranium enriched to 20% $^{235}$U or more</td>
<td></td>
<td>10 kg or more</td>
<td>Less than 10 kg but more than 1 kg</td>
</tr>
<tr>
<td></td>
<td>- uranium enriched to 10% $^{235}$U but less than 20% $^{235}$U</td>
<td></td>
<td>10 kg or more</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- uranium enriched above natural, but less than 10% $^{235}$U</td>
<td></td>
<td>10 kg or more</td>
<td></td>
</tr>
<tr>
<td>3. Uranium-233</td>
<td>Unirradiated†</td>
<td>2 kg or more</td>
<td>Less than 2 kg but more than 500 g</td>
<td>500 g or less but more than 15 g</td>
</tr>
<tr>
<td>4. Irradiated fuel</td>
<td>(The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage, and transport taking all relevant factors into account.)</td>
<td>Depleted or natural uranium, thorium or low-enriched fuel(less than 10% fissile content)$^d$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
† Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr (100 rad/hr) at one metre unshielded.
‡ Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.
§ Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.
¶ Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100 rad/hr) at one metre unshielded.
4.1.2 Nuclear Material Aggregation

During transport, different materials (plutonium, $^{233}$U and $^{235}$U with different enrichments) may be present in the same conveyance. The total amount of nuclear material on or in a conveyance should be used in determining the categorization of the conveyance and hence, identifying appropriate physical protection measures for the conveyance. There are several mathematical approaches for calculating the aggregated category for the nuclear material; a State should decide which approach it will use. (NSS-13, 6.5)

One approach is a set of aggregation formulas that are derived from Table 1 (categorization of nuclear material).

An aggregation of different materials in the same consignment should be classified as:

Category I if:

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

Category II if:

$$\frac{Pu + ^{233}U}{500} + \frac{^{235}U (\geq 20\%)}{1000} + \frac{^{235}U (\geq 10\% and < 20\%)}{10000} \geq 1 > \frac{Pu + ^{233}U}{2000} + \frac{^{235}U (\geq 20\%)}{5000}$$

Category III if:

$$\frac{Pu + ^{233}U}{15} + \frac{^{235}U (\geq 20\%)}{15} + \frac{^{235}U (\geq 10\% and < 20\%)}{1000} + \frac{^{235}U (>U_{nat} and < 10\%)}{10000} \geq 1 > \frac{Pu + ^{233}U}{500} + \frac{^{235}U (\geq 20\%)}{1000} + \frac{^{235}U (\geq 10\% and < 20\%)}{10000}$$

Below Category III if:

$$1 > \frac{Pu + ^{233}U}{15} + \frac{^{235}U (\geq 20\%)}{15} + \frac{^{235}U (\geq 10\% and < 20\%)}{1000} + \frac{^{235}U (>U_{nat} and < 10\%)}{10000}$$

or if the material consists only of $U_{natural}$ or $U_{depleted}$ or Thorium.

Where:

$Pu$ is the mass in grams of all Pu except that with isotopic composition exceeding 80% in $^{238}$Pu.

$^{233}$U is the mass in grams of $^{233}$U.

$^{235}$U (≥20%) is the mass in grams of $^{235}$U present in uranium enriched to 20% $^{235}$U or more.
$^{235}\text{U} \geq 10\% \text{ and } < 20\%$ is the mass in grams of $^{235}\text{U}$ present in uranium enriched to 10\% $^{235}\text{U}$ or more but less than 20\% $^{235}\text{U}$.

$^{235}\text{U} \text{ (}> U_{\text{nat}} \text{ and } < 10\%)$ is the mass in grams of $^{235}\text{U}$ present in uranium enriched above natural but less than 10\% $^{235}\text{U}$.

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

\[
\frac{1}{S} = \sum \frac{f_i}{S_i}
\]

where:

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

\(S_i\) (kg or g) is the mass threshold for material type \(i\) for the Category being considered

\(S\) (kg or g) is the mass threshold for the aggregation of material for the Category being considered

- The following quantities are the mass thresholds for Category I:

  - 2 kg of plutonium, all isotopes combined;
  - 5 kg of uranium 235, of uranium enriched to 20\% uranium 235 or more;
  - 2 kg of uranium 233 isotope.

- The following quantities are the mass thresholds for Category II:

  - 500 g of plutonium, all isotopes combined;
  - 1 kg of the isotope 235, of uranium enriched to 20\% uranium 235 or more;
  - 10 kg of the isotope 235, of uranium enriched to 10\% or more and less than 20\% uranium 235;
  - 500 g of uranium-233 isotope.

- The following quantities are the mass thresholds for Category III:

  - 15 g of plutonium, all isotopes combined;
  - 15 g of the isotope 235, of uranium enriched to 20\% uranium 235 or more;
- 1 kg of the isotope 235, of uranium enriched to 10% or more and less than 20% uranium 235;
- 10 kg of the isotope 235, of uranium enriched to less than 10% uranium 235;
- 15 g of uranium-233 isotope.

All plutonium isotopes and material is considered except that with isotopic concentration exceeding 80% in plutonium-238.

These thresholds relate to material that is not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy / hour (100 rad/s) at one metre unshielded.

Determining the Applicable Category

1. Determine if the aggregated material is Category I
A material, or a mixture of materials, is Category I if the aggregated mass on a conveyance is greater than or equal to the Category I mass threshold calculated for the material or mixture. If it is not Category I, proceed to step 2.

2. Determine if the aggregated material is Category II
A material, or a mixture of materials, is in Category II if the aggregated mass on a conveyance is greater than or equal to the Category II mass threshold calculated for the material or mixture. If it is not Category II, proceed to step 3.

3. Determine if the aggregated material is Category III
A material, or a mixture of materials, is in Category III if the aggregated mass on a conveyance is greater than or equal to the Category III mass threshold calculated for the material or mixture.

4. If the mass of the material or mixture of materials below the Category III mass threshold, it is "less than Category III".

Examples

- **Example 1:**

There is 5 kg of material consisting of 4 kg of uranium enriched to greater than 20% and 1 kg of plutonium. The mass fraction of uranium enriched to greater than 20% is 4/5 and for plutonium is 1/5.

Step 1.

The Category I mass threshold for this material is:

\[ \frac{1}{S} = \frac{(4/5)}{S_{U235}} + \frac{(1/5)}{S_{Pu}} = \frac{(4/5)}{5 \text{ kg}} + \frac{(1/5)}{2 \text{ kg}} \]
Then \( S = 3.84 \) kg

Since the mass of the material (5 kg) is greater than \( S \) (3.84 kg), it is above the threshold for Category I for this mixture and the shipment is Category I.

Example 2:

There is 3 kg of material consisting of 2.5 kg of uranium enriched to greater than 20% and 500 g of plutonium. The mass fraction of uranium enriched to greater than 20% is \( 2.5/3 \) (or \( 5/6 \)) and for plutonium is \( 0.5/3 \) (or \( 1/6 \)).

Step 1.

The Category I mass threshold for this material is:

\[
\frac{1}{S} = \frac{5/6}{S_{U235}} + \frac{1/6}{S_{Pu}} = \frac{5/6}{5} + \frac{1/6}{2} \text{ kg}
\]

Then \( S = 4 \) kg

The total mass is 3 kg which is below the mass threshold for the mixture for Category I.

Step 2.

The Category II mass threshold for this material is:

\[
\frac{1}{S} = \frac{5/6}{S_{U235}} + \frac{1/6}{S_{Pu}} = \frac{5/6}{1} + \frac{1/6}{0.5} \text{ kg}
\]

Then \( S = 0.86 \) kg

The total mass is 3 kg which is above the mass threshold for the mixture for Category II.

Therefore, the mixture is Category II.

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

The widespread dispersal of some nuclear materials (e.g., plutonium) in Category III (< 500 grams) or less than Category III (15 grams) could have sufficiently high consequences, that the level of protection given to prevent its acquisition for use in a nuclear explosive device is not as stringent as the level of protection that should be given to prevent its use in a radiological dispersal malicious act.

For example, 499 grams of civil industrial plutonium (the limit of Category III nuclear material) will contain about 15 000 \( A_2 \) and consequently is recommended to be protected at the "enhanced security level" for radioactive material (see “Nuclear Security Recommendations on Radioactive Material and Associated Facilities, Nuclear Security Series No. 14 (NSS-14) [8] and NSS-9). The \( A_2 \) values for
individual radionuclides are found in the Transport Regulations [6], Table 2. The enhanced security level entails more robust physical protection measures than does Category III nuclear material, such as the preparation and use of a transport security plan.

Similarly, for some nuclear materials in quantities below Category III (< 15 grams $^{233}$U or Pu), protection based on the nuclear material categorization will not be sufficient to account for their potential radiological consequences. These materials should be protected at least following the basic security level and may warrant the enhanced security level, depending on the radioactivity of the shipment and the States threat assessment.

One process for determining which physical protection measures should be applied is as follows:

1. determine the nuclear material category, taking into account all the nuclear material on board the conveyance during shipment and using the aggregation formulas if needed
   a. in the case of Category I and II nuclear material, determine the physical protection measures required based on the nuclear material category; and
   b. In the case of Category III or less than Category III nuclear material, identify the Security Level and the corresponding physical protection measures as described in the next paragraph.

2. determine the number of $A_2$ values on board the conveyance. For each radionuclide, dividing the total radioactivity (TBq) on the conveyance by the $A_2$ value (TBq) for that radionuclide will give the number of $A_2$ values for that radionuclide. Summing the number of $A_2$ values for all radionuclides with give the total number of $A_2$ values on board the conveyance. Alternatively, an effective $A_2$ value for the collection of radionuclides on board can be calculated and when divided into the total radioactivity on the conveyance will give the total number of $A_2$ values present (see paragraph 405 of the Transport Regulations).
   a. if the number of $A_2$ values equals or exceeds 3 000 the "enhanced security level" (NSS-9) should be applied to account for the radiological properties of the shipment
   b. if the number of $A_2$ values is less than 3 000 the "basic security level" (NSS-9) should be applied
   c. determine the physical protection measures required based on the nuclear material category and the radioactive material security level

3. compare the applicable physical protection measures identified in steps 1 and 2 and choose the more stringent for application to the shipment

A State may determine that an approach considering other factors may be suitable. Each categorization is used to define the physical protection measures appropriate for the risk being protected against. The most stringent of the applicable measures should be applied to a given shipment.
4.3. POTENTIAL RADIOLOGICAL CONSEQUENCES OF SABOTAGE

In addition to the physical protection measures that should be applied on the basis of the nuclear material categorization or the potential radiological consequences (section 4.2), some shipments may present significant potential radiological consequences in case of an act of sabotage. (NSS-13, 6.3)

The State should identify which shipments it believes warrant protection against sabotage due to the potential to cause unacceptable radiological consequences. States may have varying judgments on what constitutes unacceptable radiological consequences and consideration should be given to variables such as the

— package contents (radionuclides, physical and chemical forms, etc.)
— package and conveyance design
— effect of the postulated sabotage event (or events) on the contents/package/conveyance combination
— 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 8 provides additional detail on how potential radiological consequences from acts of sabotage can be determined and appropriate physical protection measures that the State might wish to require.

4.4. IDENTIFICATION OF APPLICABLE PHYSICAL PROTECTION MEASURES

The measures to protect against unauthorized removal (section 4.2 in conjunction with section 6) and sabotage (section 4.3 in conjunction with section 8) should be compared and the most stringent measures applied. In some cases there will need to be additional measures for protection against sabotage such as additional protection against standoff attacks. In other cases the measures for protection against sabotage may be of the same nature but more stringent – for example, more thorough surveillance of the route in advance of the shipment.

The State should ensure that the combination of the most stringent physical protection measures is applied to any given shipment taking into account all the properties of the nuclear material being transported.

Figure 4.1 illustrates the sequence of considerations in determining the Physical Protection measures applicable to a shipment taking into account all the potential risks of the material being transported.
Figure 4.1 Defining Physical Protection Measures to Account for All Risks
This chapter explains the provisions that the competent authority may require from a shipper, carrier and receiver and/or others as required by the State, in order to establish and maintain a sound security culture and a viable physical protection system for providing for the secure transport of nuclear material. Section 5.1 addresses different approaches Specifying and Applying Physical Protection. Section 5.2 addresses general responsibilities including specific responsibilities of shippers, carriers, and receivers for the security in transport of nuclear material. Section 5.3 discusses the key functions and objectives that may be specified by the competent authority for a physical protection system. Section 5.4 addresses the development of a TSP, including the process of submitting a TSP to a competent authority for obtaining approval, and the implementation of a TSP.

The physical protection measures for shippers, carriers and receivers recommended herein should be in addition to, and not a substitute for, other measures established for safety purposes, i.e. physical protection measures should not supplant safety measures resulting from States requirements or the IAEA Transport Regulations except where dispensation has been gained from the transport safety competent authority, for example, the use of compensatory measures for the removal of placards on high-risk shipments. (NSS-13, 3.17)

5.1. SPECIFYING AND APPLYING PHYSICAL PROTECTION

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

5.1.1 The prescriptive method

The prescriptive method allows the competent authority to establish specific physical protection measures to meet its defined physical protection objectives for each category of nuclear material. It provides a set of recommended “baseline” provisions for the shipper/carry to apply for the transport of each category. A set of recommended “baseline” provisions is provided in Section 6.

Advantages of the prescriptive method include: simplicity in implementation for both the competent authority and the shipper/carry; elimination of the need to transmit sensitive information in the form of results of a threat assessment or DBT; and ease of inspection and auditing.

The disadvantage of the prescriptive method is its relative lack of flexibility in addressing actual circumstances. The use of the prescriptive method may be particularly appropriate in cases where the
combination of threat and potential consequences is low. For example, where shipments of category III nuclear material take place in a relatively stable socio-political environment, or where conducting a detailed threat assessment and establishing a State DBT is not practical or possible.

5.1.2 The performance-based method

The security provisions used in the performance-based approach are based on the overall objectives of the security system that are defined by the competent authority. In the performance based approach, the competent authority defines the security objectives to be met on the basis of a national threat assessment and, where applicable, a DBT.

The performance based approach allows flexibility for the operator to propose a particular combination of physical protection measures. The adequacy of these measures is then assessed against the TA or DBT. This will ensure that performance based measures meet the set objectives and provide an analysis of the physical protection system designed to satisfy the five key functions of deter, detect, assess, delay and response to a malicious act.

The advantages of this approach are that it recognizes that an effective security system can be composed of many combinations of physical protection measures, and that each operator’s circumstances can be unique. The performance based approach is also the most cost effective approach for a knowledgeable Shipper or carrier.

The disadvantages of this approach are that it requires both the operator and the regulatory body to have relatively high levels of security expertise and that the competent authority must divulge some sensitive information from the State’s threat assessment or DBT to the shipper or carrier and that the shipper or carrier must have capabilities to provide adequate protection of this sensitive information.

5.1.3 The combined method

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

— The competent authority could require application of a performance-based method for the nuclear materials in transport having the highest potential consequences of malicious use, while allowing application of a prescriptive method for lower consequence nuclear materials in transport.

— The competent authority may require that a set of prescriptive requirements be supplemented by using the performance based method to address particular matters such as the current threat.
The competent authority may adopt a large set of physical protection measures from which the shipper may choose, requiring the shipper to demonstrate that its resulting security system, as a whole, meets the applicable State physical protection objectives.

The main advantage of the combined method is the flexibility it allows. It potentially adds a smaller burden on both the State’s competent authority and the shipper since it can utilize provisions from the prescriptive method as a baseline, while coupling it with knowledge of threats. Following the assessment of the threats by a State, the competent authority can then provide requirements based on modifications, as determined appropriate, of the baseline provisions.

The disadvantages of the performance-based elements of the combined approach will be similar to those associated with the performance-based approach.

### 5.1.4 Process for Applying the Methods

The process that a State may follow in deciding which method to use is shown in Figure 5.1. The figure highlights the decisions that need to be made by the competent authority regarding which method to use, and if the combined method is chosen, the decision of specifying which option is to be used for each category of nuclear material.
Fig. 5.1: Decision process for determining the Regulatory Approach to Transport Security.

5.2. GENERAL RESPONSIBILITIES FOR PHYSICAL PROTECTION IN TRANSPORT

Assignment of physical protection responsibilities for the planning and completion of nuclear material transports should be clearly defined by the State or its competent authority. This will vary from State to State. General responsibilities that the State may assign include developing a TSP, providing advance notification of the shipment details to the receiver and completing other relevant technical, procedural and administrative activities. In addition to these general responsibilities, there are also specific responsibilities that can only be completed by the shipper, carrier or receiver.

The entity responsible for physical protection of the shipment (generally the shipper or carrier) should develop a TSP in accordance with the State’s regulatory framework. Information on how to develop a TSP can be found in Section 5.4 of this publication.

In accordance with the States regulatory framework, the entity responsible should give the receiver advance notification of the shipment details and the expected time of arrival, and follow up with details of any unexpected change.
5.2.1 Specific Responsibilities for Shipper

Prior to transporting nuclear material, the shipper should ensure that all the necessary permits and authorizations have been obtained. If also responsible for physical protection, the shipper should ensure that all measures and arrangements for security of the shipment are in place. If handing over to a carrier who is responsible for physical protection, the shipper should ensure that the carrier concerned is authorized to transport nuclear material.

5.2.2 Responsibilities for Shipper/Carrier

Prior to commencing transport, the shipper/carrier should verify that all physical protection measures are in accordance with the TSP. If it is determined that the physical protection measures do not provide the required level of protection described in the TSP, the shipper/carrier should immediately correct the situation, inform the competent authority and, if necessary, postpone the shipment. (NSS No13, 3.30 and 6.23)

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

The shipper/carrier should conduct inspections of the conveyance prior to commencing transport, after any stops (scheduled and unscheduled) and on arrival to its destination. This will allow the shipper/carrier to determine any loss of or damage to, or tampering of, packages during transport and on delivery. Further information on inspections and searches can be found in Section 6.1.8 of this publication.

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

5.2.3 Specific Responsibilities for Receiver

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

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

5.3. KEY FUNCTIONS AND OBJECTIVES OF A PHYSICAL PROTECTION SYSTEM

Shipments of nuclear material need in-depth protection against unauthorized removal, sabotage and other intentional malicious acts. The key functions of physical protection include deter; detect; assess;
delay; and respond. These fundamental concepts apply to all categories of nuclear material; however, their implementation should be accomplished in a graded manner and considered in the context of the States threat assessment

5.3.1 Deter
Transport physical protection measures should include features that are visible and are intended to deter malicious acts. These features could include visible physical protection measures built into the conveyance, the use of guards, convoys etc. These measures may also perform other physical protection functions. However, they should not affect the safety design of the package

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

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

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

5.3.4 Delay
Physical protection measures in transport should provide sufficient delay to those with malicious intent to enable an appropriate and effective response. The amount of delay required will depend on the amount of time required for a response force to respond and should be applied in a graded manor taking in to account the category of the nuclear material.

5.3.5 Respond
The response to a security event may come from accompanying guards or other local or regional authorities. Response activities should encompass the objectives to mitigate or minimise a malicious act and locate and recover missing material.
5.4. DEVELOPING THE TRANSPORT SECURITY PLAN

The TSP should document all physical protection measures and arrangements necessary to adequately address the requirements and/or objectives of the competent authority. By following the guidelines set forth in this publication, the TSP will identify responsibilities for all aspects of the protection of nuclear material in transport. The competent authority determines who is responsible to submit the TSP. This will normally be the shipper or carrier having direct responsibility for the security of the nuclear material in any particular mode or phase of the transport.

An assessment of potential vulnerabilities prior to a shipment takes into account all information, as appropriate, regarding the mode or modes of transport; the route to be followed; any transit sites, stopover points, temporary storage or transfer areas, and planned or potential stopping places. Other parts of the transport system that affects its vulnerability includes the conveyances, equipment and personnel involved in the shipment; the capabilities of the transport control centre, the response force; and the operating conditions during transport. The result of this assessment is then used to assess the effectiveness of the shipper or carrier’s physical protection system in one or more scenarios that represent a probable security event, and to make a judgment as to whether the overall effectiveness of the physical protection system is adequate or if improvements such as compensatory measures are needed.

In-transit storage and inter-modal transfers – If road movements cannot be completed without overnight or extended stops, or if there is a requirement to place nuclear material in temporary storage while en route (for instance at a transfer point), then the nuclear material should be protected during such stops or storage in a manner that is consistent with storage measures that would be employed at a nuclear facility, to the extent practicable and consistent with the potential consequence of a malicious act against the material. For shipments of Category I and Category II nuclear material, a temporary protected area could be established (or an existing protected area such as at a nuclear facility or military base could be used) to which access is restricted and which is under surveillance by guards that is in close communication with response forces. If the material is to remain on the vehicle during road shipment layovers then the vehicle should be immobilised in order to deter or delay any unauthorised movement. Temporary storage arrangements should be approved in advance by the competent authority as part of the TSP.

TSP should also include the procedures for reporting non-compliances during the transport by the shipper/carerrier to the competent authority [NSS-15].

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). The TSP can be divided into several parts and only the relevant parts shared with organizations.
5.4.1 Submitting and Obtaining Approval of the Transport Security Plan

The State will specify whether a shipper’s/carrier’s TSP and any associated vulnerability assessment requires submission to the competent authority for review and approval. This may depend upon the category of material being proposed for transport. Thus, the TSP, along with the vulnerability assessment if one is required, should be submitted to the competent authority or other approval organizations, as designated by the State. This activity could be an iterative process. If the competent authority feels that the State Requirements are not met in the TSP or that the results of the vulnerability assessment are inadequate, the TSP and/or vulnerability assessment should be returned to the originator for additional information and action.

For transports of all Category I and II materials TSP should be submitted by the shipper/carerrier, to the competent authority for approval. A plan may cover a series of similar movements.

The process of developing and, when required, submitting and obtaining approval of a TSP is depicted graphically in Figure 5.2.
Fig. 5.2: Sample process for Competent Authority review and approval of a vulnerability assessment, if needed, and a Transport Security Plan.

5.4.2 Implementing the Transport Security Plan

Once the TSP, and if required the vulnerability assessment, have been submitted and when required, approved by the competent authority, detailed plans and preparations for the shipment can proceed. Physical protection of the shipment should be undertaken in accordance with the approved TSP and associated written instructions and agreements. If for any reason the shipment cannot be completed in accordance with the TSP, the shipper/carry should immediately implement compensatory measure to maintain the level of protection and inform the competent authority as soon as is practicable. The
competent authority may require the shipper/carrier to prepare a set of compensatory measures in advance. (NSS No 13, 3.30)

If any incidents or unscheduled delays have occurred during transport, a review of physical protection 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.
6. MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN TRANSPORT

In accordance with the graded approach, the shipment of all nuclear material includes physical security during all phases of the transport operation. The specific physical protection measures will change depending on which category of nuclear material is being shipped starting with common requirements that should be applied to all shipments of nuclear material followed by requirements (in increasing order of stringency) for Category III, II and I nuclear material. The provisions recommended for lower levels are additive to the next higher level category.

This section recommends a set of provisions that a State should consider when defining transport security requirements for all categories of nuclear material.

The measures described in this section should be treated as baseline measures by the competent authority. In specific areas the competent authority may wish to add to these provisions for the category of material being transported, or to define the State’s physical protection requirements in more detail than is done in NSS-13. In all cases, the competent authority should take account of the level of attractiveness of the nuclear material, the potential threat posed to the shipment, local circumstances and the results of the State’s threat assessments and/or a DBT. Increased physical protection measures, above those shown in this section, may be required particularly if additional sabotage protection is determined to be required (see Section 8).

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

The provisions in this section are specified by topic to allow emphasis to be placed upon the graded approach for establishing a physical security system to protect against unauthorised removal. Physical protection measures against sabotage are described in section 8.

Section 6.1 presents recommended provisions, specified by category of material to be transported, independent of the mode of transport, Section 6.2 provides recommended provisions that are mode dependent, Section 6.3 includes recommended provisions for international transport, and Section 6.4
presents additional physical protection measures based on potential radiological consequences from unauthorised removal and subsequent dispersion. Each third-level subsection deals with a specific function, defining recommended provisions beginning with Category III nuclear material, and then moving to higher level categories imposing more stringent recommended provisions. If the same provisions are recommended for all three categories, they are so noted. The competent authority, at its discretion and as deemed appropriate, may modify, increase or eliminate specific provisions for a given level of protection afforded to any category of material being transported.

6.1. MODE INDEPENDENT PROVISIONS

The State has responsibility to ensure prudent management practices are applied during transport for all nuclear material, including:

(a) quantities of nuclear material less than Category III,
(b) natural uranium, depleted uranium and thorium, and
(c) nuclear material which is in a form that is no longer usable for any nuclear activity, minimizes environmental dispersal and is practicably irrecoverable. (NSS No,13, Table 1 footnote c and 4.7)

Prudent management practices include those normal commercial practices implemented by shippers and carriers to protect the material being shipped as an asset. These include accepting responsibility for the safe keeping of the material while it is under their control and protecting it against loss or theft in a manner commensurate with its value. The material must 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 unauthorised removal.

6.1.1 Common Requirements

There are several "common requirements for transport of nuclear material" (NSS-13 Section 6) that should be considered when planning and making shipments. When applying these recommendations, the State should be pragmatic when implementing the "graded approach" and "as far as operationally practicable" – particularly for shipment of material that is less than Category III or in Category III. These types of material are typically transported by commercial carriers under non-exclusive use conditions and the practicalities of commercial shipping should be considered in light of the limited risks posed by the lower category materials. For Category II and Category I the common requirements should be applied more rigorously.
Physical protection against unauthorized removal during all nuclear material transport should encompass, as far as operationally practicable in accordance with the graded approach (NSS-13, 6.6):

a. Minimizing the total time during which the nuclear material remains in transport;

This helps minimize the time during which the material is outside a protected facility and the time during which an adversary might attempt to obtain it while in transport.

b. Minimizing the number and duration of nuclear material transfers, i.e. transfer from one conveyance to another, transfer to and from temporary storage and temporary storage while awaiting the arrival of a conveyance, etc.;

c. Protecting nuclear material during transport and in temporary storage in a manner consistent with the category of that nuclear material;

d. Avoiding the use of predictable movement schedules by varying times and routes;

Rail, ocean and air movements may require use of regularly scheduled conveyances but predictable shipment patterns should be avoided if possible.

e. Requiring predetermination of the trustworthiness of individuals involved in transport of nuclear material;

For shipments of smaller quantities of nuclear material, consideration may be given to the normal security vetting applied to transport employees involved in transporting dangerous or valuable goods. Considering the wide range of persons involved in transport activities including international transport, the States should apply a graded and flexibilities approach in the determination of its trustworthiness policy, commensurate with the State laws and regulations. (NSS-13, 3.14)

f. Limiting advance knowledge of transport information to the minimum number of persons necessary;

g. Using a material transport system with passive and/or active physical protection measures appropriate for the threat assessment or design basis threat;

For shipments of smaller quantities of nuclear material, consideration may be given to the protection afforded by the conveyances normally used by the carriers (e.g. vehicles with locked cargo compartments).

h. Using routes which avoid areas of natural disaster, civil disorder or with a known threat; and,

i. Ensuring that packages and/or conveyance are not left unattended for any longer than is absolutely necessary.
A State may determine that certain categories of nuclear material require continuous surveillance. Shipments of smaller quantities of nuclear material using non-exclusive use conveyances may not be continuously attended (e.g. when the driver is making a delivery) but the time they are unattended is normally minimized.

When a series of shipments is planned by a shipper, the number and nature of the shipments should be optimized to ensure that security is not compromised for operational convenience. For example, it may be tempting for a shipper to make a series of Category III shipments rather than a single Category II shipment. However, consideration must be given to the prevailing threat, resources available to deal with potentially simultaneous nuclear security events and the amount of material in transit at any given time.

### 6.1.2. Selection of Mode and Routing

#### 6.1.2.1 Provisions for Category I and II nuclear material

In determining the mode or modes of transport and routing to be used in the transport of nuclear material, the shipper should identify and evaluate the characteristics of the proposed shipment relative to their impacts on the ability to protect the shipment against the potential threats involved. These methods and or requirements for these determinations should be established by the competent authority, and should also be based on any relevant State threat assessments s, and/or DBT, and any shipper’s vulnerability assessments if required by the competent authority. The mode of transport for any given consignment should be such as to keep to a minimum the number of cargo transfers and the length of time the cargo remains in transit.

The TSP should identify the mode(s) and route(s) of the transport. When the use of alternate routes may be necessary, the TSP should identify the alternate routes and the conditions under which those routes would be used. (NSS 13, 6.22) In choosing the route and mode consideration should be given to:

1. the security situation along the entire route – e.g. avoiding known threat areas or areas where security cannot be assured
2. political and international dynamics along potential routes
3. response force capabilities and the time require for response forces to reach any point along the route
4. practicality of the route, including acceptance/approval by transit countries and their ability and willingness to ensure security during transit through their country
6.1.2.2 Additional provisions for Category I nuclear material

When operationally practicable, the use of rail transport should be avoided or at least minimized due to limited routing options, predictability of routes and possible long distances from response forces (i.e., long response times).

6.1.3 Assessment and Approval of the Transport Security Plan

6.1.3.1 Provisions for Category I and II nuclear material

The competent authority should require that a TSP be developed and submitted for approval. The TSP may be developed and submitted by the shipper and/or the carrier, depending on whom the competent authority assigns these responsibilities to. As part of this process, the competent authority should define the content of the TSP, the process for submitting it and how any revisions required by the competent authority should be incorporated. Threat assessment should be an integral part of the TSP development and review process. The competent authority has discretion in whether or not it issues formal approval of a TSP for Category II material. (NSS-13, 6.22)

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

The required content of the TSP should be specified in detail. Topics that may require detailed descriptions in the TSP include: training and exercises; pre-operational testing of physical protection equipment trustworthiness verification; physical protection measures; emergency and contingency plans; trans-shipment points and intermodal transfers. For international shipments, references should be made to any intergovernmental agreements governing responsibilities and transfer of responsibilities. Additional details on the content of the TSP are provided in Annex II.

As a result of its review of the TSP, the competent authority may identify parts of the plan that it feels warrant exercises to evaluate the adequacy of the security arrangements. The competent authority should then ensure that the exercises are completed, results documented and any needed improvements identified and that any necessary changes are incorporated into the TSP. Similarly, the competent authority may require that vulnerability assessments be performed on any parts of the plan that it feels warrant more detailed analysis, such as stopping points, route selection and intermodal transfer points.

Information in the TSP will be sensitive, particularly information on the route and schedule of shipments. This information should be identified, marked and handled in accordance with the competent authority requirements for sensitive information.
6.1.3.2 Provisions for Category I nuclear material

The approval by the competent authority of the TSP should be based on a detailed examination of proposed physical protection measures, which should provide sufficient delay so that guards and/or response forces have time to intervene to prevent unauthorized removal. The competent authority should approve the mode and route of transport proposed in the TSP, including any alternate route, arrangements and conditions for using alternate routes, stopover facilities and inter-modal transfers. The TSP should include arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, threat assessment and operating conditions (NSS-13, 6.33).

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

6.1.4. Authorization of Shipments

6.1.4.1 Provisions for Category I nuclear material

Authorization by the competent authority for the shipment should be required just prior to commencing transport and should be conditional on current threat assessment and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment. The consent to a transport operation can include specific limitations and conditions related to the particular circumstances. (NSS-13, 6.34)

The competent authority should specify what information is required to be submitted in order to receive a shipment authorization and the process for obtaining the authorization. In its evaluation of a request for shipment authorization, the competent authority should:

1. review the latest threat information and conditions along the route to ensure that the measures required by the TSP will still provide adequate security during the transport
2. verify that personnel and transport arrangements have not changed in a way that would adversely affect security
3. consider the need to require verification of equipment (presence and functionality) and transport arrangements immediately prior to dispatch of the shipment. This can be in the form of a readiness review which may be complemented with an inspection conducted by the competent authority

55
6.1.5.  Advance Notification and Coordination

6.1.5.1 Provisions for Category I, II and III nuclear material

The shipper/carrier should give the receiver advance notification of the planned shipment specifying
the mode of transport (road/rail/water/air), the estimated time of arrival of the shipment and the exact
point of hand-over if this is to be done at some intermediate point before the ultimate destination. This
advance notification should be supplied in time to enable the receiver to make adequate physical
protection arrangements (NSS-13, 6.12).

Physical protection in transport should include prior agreement among the shipper, receiver and
carrier. Such agreement may be based on normal commercial practices and responsibilities.
Agreement should exist on the time, place and procedures for transferring physical protection
responsibilities – for example, this could be when the shipment is released to the carrier. (NSS-13, 6.13)

Carriers should only transfer nuclear material packages to other carriers that are known to them to be
bona fide carriers. In the case of transports using foreign based carriers, the suitability of those
carriers should be confirmed with the State authorities. The suitability of foreign based carriers may
be confirmed by consideration of that carrier’s experience with similar transports or information
exchange with the competent authorities of that State.

6.1.5.2 Additional Provisions for Category I and II nuclear material

The receiver should confirm readiness to accept the delivery (and handover as applicable) at the
expected time, prior to the commencement of the shipment. In some cases formal agreements may be
required and these should be strictly followed. It is particularly important that transport schedules be
maintained where these agreements are involved. (NSS-13, 6.21)

6.1.6.  Locks, Seals, Alarms and Engineered Systems

6.1.6.1 Provisions for Category I, II and III nuclear material

In compliance with transport safety requirements, the outside of every package containing nuclear
material should incorporate a feature such as a seal, which is not readily breakable and which, while
intact, will be evidence that it has not been opened. However, most seals do not provide intrusion
detection capability – they only indicate that intrusion has occurred and only when they are physically
checked. Seals should not be viewed as a substitute for intrusion detection and/or surveillance.

Packages containing nuclear material should be carried in closed, locked conveyances, compartments
or freight containers. However, carriage of packages weighing more than 2000 kg that are locked or
sealed may be allowed in open vehicles. Packages should be tied down or attached to the vehicle or
freight container and should be secured as appropriate. Whenever it is necessary to use open
conveyances, the load should be covered or hidden from view unless safety requirements preclude this. (NSS-13, 6.14)

Where practicable, locks and seals commensurate with the categorization of the nuclear material being transported should be applied to conveyances, compartments or freight containers. If locks and/or seals are used, checks should be made before dispatch and during any intermodal transfer of each nuclear material consignment to confirm the integrity of the locks and seals on the package, vehicle, compartment or freight container. When enclosed freight containers are used, verification of the integrity of a door seal should be sufficient in lieu of verifying each individual seal on packages inside the freight container. (NSS-13, 6.15)

Procedures should be established to ensure the security of keys to conveyances and security locks commensurate with the categorization of the nuclear material being transported. (NSS-13, 6.9)

The receiver should check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver should notify the shipper of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at the destination. (NSS-13, 6.18)

The security level of locks should follow the graded approach, based on the category of the package. Lock fittings and components, such as attachment points and tie downs, should be complimentary to the quality and strength of the required locks.

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

6.1.6.2 Additional provisions for Category I and II nuclear material

The physical protection measures applied to the transport system (conveyance, freight container and/or package) should include delay measures to increase the time required by an adversary to complete an unauthorized removal of the nuclear material. The delay should be sufficient to allow guards and/or response forces the time needed to make an appropriate response. (NSS-13, 6.25)

Requiring the use of electronic intrusion detection and duress alarms should be considered.

High strength and high security locks should be required on packages for Category I and II materials.
6.1.6.3 Additional provisions for Category I nuclear material

The physical protection measures applied to the transport system (conveyance, freight container and/or package) should include delay measures to increase the time required by an adversary to complete a malicious act. The delay should be sufficient to allow guards and/or response forces the time needed to prevent unauthorized removal of the nuclear material. (NSS-13, 6.25)

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

When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, enhanced physical protection measures should be applied, such as additional guards. The package should be tied down or attached to the conveyance or freight container with multiple locking mechanisms that require to be unlocked by two different keys held by two different authorized persons, also known as the “two person rule” The locking devices should not interfere with the safety performance of the package (NSS-13, 6.36)

6.1.7. Written Instructions

6.1.7.1 Provisions for Category I, II and III nuclear material

The shipper or carrier should provide consignment-specific transport documents to appropriate carrier personnel. These documents should include information regarding actions that are required to be taken in the event of an accident or security event that has not already been covered in prior training or instructions. During transport, drivers or operators of the conveyance should be given emergency contact information for the countries being transited. The information may be part of other instructions or manuals, such as shipboard emergency procedures. The documents should be provided in the languages deemed necessary by the shipper, carrier or the authorities concerned and should be appropriately controlled.

6.1.7.2 Additional provisions for Category I and II nuclear material

Written instructions detailing physical protection responsibilities (consistent with the TSP) should be provided in advance of the shipment to all personnel with such responsibilities. If the competent authority requires approval of those instructions, they should be reviewed and approved by the competent authority. The content of the instructions and the procedure for approval should be specified by the competent authority. Alternatively, the competent authority may require that the shipper or carrier issue them. (NSS-13, 6.27)
6.1.7.3 Additional provisions for Category I nuclear material

Written instructions detailing physical protection responsibilities, including responsibilities of all transport control centre or alternate central point of communication, carrier, guards and response force personnel should be appropriately classified and provided in advance of the shipment to personnel with those physical protection responsibilities.

6.1.8. Inspections, Searches and Surveillance

6.1.8.1 Provisions for Category I, II and III nuclear material

There should be a detailed search of the conveyance to ensure that nothing has been tampered with and that nothing has been affixed to the package or conveyance that might compromise the security of the consignment. Shipper/carryer personnel should undertake periodic inspections and security searches at appropriate times, including after loading but before dispatch and during transport, verifying that all specified physical protection measures on the load carrying conveyances are effective. In many cases it will be sufficient for the carrier to perform a visual inspection based on their own knowledge of the conveyance. (NSS-13, 6.16)

6.1.8.2 Additional provisions for Category I and II nuclear material

The conveyance should be searched immediately prior to loading and shipment. This may require appropriately trained personnel to ensure that the conveyance has not been tampered with in any way. Immediately following completion of the search, the conveyance should be placed in a secure area or kept under guard surveillance pending its loading and shipment for transport and unloading. (NSS-13, 6.26)

Prior to commencing transport, the carrier should verify that all physical protection measures are in place and are functioning normally in accordance with the TSP. (NSS-13, 6.23)

Inspections should be made before dispatch of each nuclear material consignment to confirm the integrity of the locks and seals on the package, freight container, compartment, or conveyance. These inspections should be undertaken in accordance with information and procedures provided in the TSP.

Physical protection measures should include continuous and effective surveillance of the cargo, load compartment or conveyance. States are encouraged to use guards for such surveillance. Surveillance may include use of remote technologies such as closed circuit television and detection technologies such as video motion detection. (NSS-13, 6.20) The guards should respond to any anomalies reported as part of the surveillance activity.

6.1.8.3 Additional provisions for Category I nuclear material

Security inspections should be performed on all equipment, stores, personal effects and other goods loaded onto the conveyance.
Guards and escorts providing surveillance should do so under conditions which ensure close communication with response forces.

6.1.9. Communication and Confidentiality Involving the Shipper, Carriers and Receiver

6.1.9.1 Provisions for Category I, II and III nuclear material

A method for periodically identifying the location (e.g. using bar-code tracking systems) of a consignment of nuclear material should be considered. Information concerning the location of the consignment should be properly controlled and should be readily available to the shipper and/or carrier and should be provided to the receiver when appropriate.

6.1.9.2 Additional provisions for Category I and II nuclear material

A method for providing positional tracking (e.g. satellite-based tracking systems) of a consignment of nuclear material should be considered.

Consideration should be given to establishing a transport control centre or a less robust alternative central point of communication as a central location to monitor and coordinate voice and/or digital communication traffic between personnel involved with a specific shipment or group of shipments, to monitor positional tracking, and to facilitate command and control.

Physical protection measures should include provision of continuous two-way voice communication between the conveyance, any guards accompanying the shipment, the designated response forces and, where appropriate, the shipper and/or receiver. (NSS-13, 6.29)

6.1.9.3 Additional provisions for Category I nuclear material

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

The transport control centre should be protected so that its function can continue in the presence of the threat. It should be physically protected from attack, provide for access control for staff and other authorized personnel, and be alarmed with a monitored security system. While the shipment is in progress, the transport control centre should be staffed by qualified personnel and any other personnel designated by the competent authority whose trustworthiness has been predetermined. (NSS-13, 6.37)

The transport control centre should utilize redundant communications channels and be equipped with emergency electrical power. Communications equipment is subject to interference, jamming, lost signals, and gaps in coverage. By incorporating multiple communications systems using different equipment, frequencies, and technologies, these limitations can be mitigated. No communications
channel can ensure complete information security, but the use of encryption technologies, coding or
secure channels can counteract monitoring and make real-time interception and monitoring extremely
difficult.

The level of capability of each transport control centre should be matched to the size and complexity
of the transport operations, the anticipated threats, the communications needs of the response
organizations, and the existing communications infrastructure of the Member State(s). Continuous
two-way communication systems between the conveyance, transport control centre, guards
accompanying the shipment, the designated response forces, and where appropriate, the shipper
and/or receiver should be redundant, diverse and secure. (NSS-13, 6.38)

An individual should be designated in the TSP with the responsibility to report to the transport control
centre on the arrival of the shipment at each stopover facility and any completion of hand-over of
responsibility of the shipment. This communication should be performed in accordance with the TSP.
(NSS-13, 6.39)

6.1.10. Guards

Arrangements should be made to provide sufficient guards and/or response forces to deal with nuclear
security events consistent with the category of nuclear material being transported and physical
protection measures should include communication from the conveyance capable of summoning
appropriate responders. The graded approach, based on the category of the nuclear material, should be
used in specifying the physical protection measures necessary to accomplish this. For example, for
lower category material accompanying guards may not be necessary if the competent authority
determines that response forces are sufficient. (NSS-13, 6.17)

6.1.10.1 Provisions for Category I, II and III nuclear material

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

6.1.10.2 Additional provisions for Category I and II nuclear material

When justified by the State’s threat assessment, States are encouraged to use armed guards for
shipments of Category II nuclear material to the extent that laws and regulations permit. If guards are
not armed, compensating measures should be applied such as additional monitoring and delay
features. (NSS-13, 6.24)
6.1.10.3 Additional Provisions for Category I nuclear material

Guards, appropriately equipped and trained, should accompany each shipment to protect the nuclear material, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the guard at all times, especially when the conveyance is not in motion. The guards should respond to any anomalies reported as part of the surveillance activities. States are encouraged to use armed guards to the extent that laws and regulations permit. When guards are not armed, compensating measures should be applied, such as adding delay barriers to the conveyance exterior structure and/or interior cargo area and less-than-lethal incapacitating agents. Guards capabilities should be established with due consideration of the number of load carrying conveyances in the transport operation. (NSS-13, 6.35)

The guards or conveyance crew should be instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of hand-over of the shipment by secure two-way voice communications to the transport control centre. (NSS-13, 6.39)

6.1.11. Response Forces and Emergency Actions

6.1.11.1 Provisions for Category I, II and III nuclear material

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

6.1.11.2 Additional provisions for Category I and II nuclear material

Arrangements should be considered, as appropriate, for providing adequately sized, equipped and trained response forces to deal with emergencies that may arise during transport of Category II nuclear material.

Arrangements should be made to provide adequately sized response forces to deal with nuclear security events. The objective should be the arrival of the response forces in time to prevent the unauthorized removal (NSS-13, 6.30). In accordance with the graded approach, the competent authority may allow differences in the size and capabilities of response forces for Category I and Category II material. Similarly, the extent to which there is assurance that unauthorized removal will be prevented (system effectiveness) may also vary between the two categories.

6.1.11.3 Additional provisions for Category I nuclear material

Arrangements should be made to provide adequately sized, equipped and trained response forces to deal with emergencies that may arise during transport of Category I nuclear material. The response force should be adequately staffed and trained, and capable of arriving at any location of an accident...
or an adversarial action in time to prevent the unauthorized removal of nuclear material. The response force should be capable of locating and recovering nuclear material should an adversary gain control of it.

Based on the State's assessment of the threat, if the guards have sufficient capability to counter the threat, a dedicated response force may not be necessary.

6.1.12. Measures after Transport

6.1.12.1 Provisions for Category I, II and III nuclear material

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

The receiver should notify the shipper, the carrier, and the competent authority of the non-arrival of a shipment in the event that the shipment does not arrive at its intended destination after an interval of time agreed to in advance by the shipper, receiver and – as appropriate – the competent authority.

Any deficiencies in the physical protection system noted during transport should be corrected before any subsequent transport is undertaken and reported to the competent authority.

6.1.12.2 Additional provisions for Category I nuclear material

The person authorized in the TSP should report to the transport control centre, by appropriate communications in accordance with information provided in its TSP, the arrival of the consignment at its destination and the completion of the hand-over of the shipment.

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

6.1.13. Unplanned Stops

If the conveyance makes an unexpected extended stop, the physical protection measures appropriate for that category of material in storage should be applied to the extent possible and practicable. Physical protection of nuclear material in storage incidental to transport should be at a level appropriate for the category of the nuclear material and provide a level of protection consistent with that required for nuclear material in use and storage. (NSS-13, 6.10)
6.1.14 Information Security

Appropriate measures, consistent with national requirements and using a graded approach, should be taken to protect the confidentiality of information relating to transport operations, based on a need to know, including detailed information on the schedule and route. (NSS-13, 6.7). Consideration should be given to providing adequate protection to a range of sensitive information related to transport. Such information includes the physical protection measures including capability of the response force, the detection, assessment and delay capabilities etc. In addition, computer security is critical to protecting sensitive information, particularly for a transport control centre. Measures should be taken to ensure the security of all electronic systems, particularly computer systems.

It is highly recommended to ensure as far as possible the “unpredictability” of shipments in order to make it difficult for an adversary to effectively plan an attack. Consequently, information on routes and schedules is particularly sensitive and should be protected accordingly. Great restraint should be applied in the use of any special markings on conveyances, and also in the use of open channels for transmission of messages concerning shipments of nuclear material. (NSS-13, 6.7) In many cases, the external markings (i.e. placards) on conveyances are to alert emergency responders of the presence of radioactive material. Alternate measures may be used to accomplish this function, such as accompanying emergency response personnel or communications arrangements that would allow transmission of this information in case of an accident. When alternate measures acceptable to the transport safety competent authority are in place, the external markings may not be necessary.

When a security-related message is transmitted, measures such as coding and appropriate routing should be taken to the extent practicable, and care should be exercised in the handling of such information. (NSS-13, 6.7)

6.2. MODE SPECIFIC PROVISIONS

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

6.2.1. Additional Provisions for Road Transport

6.2.1.1 Additional provisions for Category I, II and III nuclear material

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

Transports of nuclear material by road should be on conveyances operated under exclusive use conditions. (NSS-13, 6.31)

For shipments of Category I and Category II nuclear material, a temporary protected area could be established (or an existing protected area such as at a nuclear facility or military base could be used) to which access is restricted and which is under surveillance by guards that are in close communication with response forces. For the road movements, if the material is to remain on the load carrying vehicle, then the vehicle should be secured in order to deter or delay any unauthorized movement. Temporary storage arrangements should be approved in advance by the competent authority as part of the TSP.

Prior arrangements should be made for overnight stay at an appropriately equipped and secured road stopover facility if the road transport cannot be completed, uninterrupted. During such stays the load carrying road vehicle should be immobilized and guarded or parked in a secure locked and guarded building or facility. Planned stopover locations and arrangements should be arranged in advance.

6.2.1.3 Additional Provisions for Category I nuclear material

Consignments of Category I nuclear material should be transported on conveyances (a) specifically designed to resist attack by equipping them with technical measures to detect, deter, and delay access to the shipment, and (b) equipped with a vehicle disabling device. A guard or crew member, in addition to the driver, with formal security responsibilities should travel in each load carrying vehicle. The vehicle driver and accompanying person should be capable of activating the response according to the TSP (NSS-13, 6.40).

Each load carrying vehicle should be accompanied by a minimum of one accompanying vehicle manned by guard members. Adequate, protected communication between all vehicles in the convoy should be provided. Accompanying guards should conduct a surveillance of the route for any threat indicators, protect the conveyance and be prepared to initiate an appropriate response Route surveillance may also be performed from an unmarked vehicle traveling some distance in front of the conveyance and escort vehicle. Surveillance may also be performed from aircraft (NSS-13, 6.40).

Consideration may also be given to (a) limiting the number of load carrying transport vehicles used in any one convoy; (b) utilizing a lead reconnaissance vehicle that travels in advance of the convoy to assess route situations, raise alarms as needed, possibly redirect the convoy, and initiate response force actions as needed; (c) having a minimum of two people travel in each vehicle in the convoy where each person would be capable of detecting and responding to an unauthorized action of the other.
Because of the need to prevent tampering and protect design information of the physical protection equipment, even when empty the conveyance should be protected from unauthorized access or observation.

For road shipments, safe havens should be identified along the route during the planning process that can be utilized during emergencies or other unplanned stops.

For road shipments of Category I material, the transport vehicle should be equipped with features approved by the competent authority that permit immobilization of the cab or cargo-carrying portion of the vehicle. This requirement applies equally to all transport vehicles used in a single shipment. In this requirement, immobilization means rendering the loaded transport vehicle incapable of movement under its own power. The purpose of this requirement is to deny an adversary who may succeed in gaining control of a transport vehicle the ability to move or flee with the vehicle. The immobilization technique should be implemented only when it is apparent that an attempt is being made to gain unauthorized control over the shipment. Immobilization should not be initiated in a way that would endanger the driver, escorts, or members of the public. Immobilization procedures should be developed and incorporated into the TSP. Operation of the immobilization technique and the procedures governing its use must be covered in the training for escorts and for drivers. The immobilization techniques should meet each of the following criteria:

— The immobilization device and procedure can be operated and performed from inside the cab of the transport vehicle by one person.
— Immobilization should be accomplished in a short period of time (several seconds) after the immobilization procedures are initiated.
— After immobilization is accomplished, skilled technical personnel should require at least the response time to return the transport vehicle to normal operating conditions. It should not be possible, by coercion of the drivers or escorts, for an adversary to bypass the effects of the immobilization or to significantly shorten the time needed to make the transport operational again.
— The device should pose no significant safety hazard before, during, or after the immobilization.

Devices employed to effect immobilization may be mechanical or electrical. They should be relatively simple and reliable to operate, so that they can be activated quickly under stressful conditions.
6.2.2. Additional Provisions for Rail Transport

6.2.2.1 Additional provisions for Category I, II and III nuclear material

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

6.2.2.2 Additional provisions for Category I and II nuclear material

Packages containing Category I and II nuclear material should be carried in exclusive use, enclosed, locked rail vehicles or freight containers unless precluded by overriding safety considerations.(NSS-13, 6.31)

Prior arrangements should be made for stay at an appropriately equipped and secured rail stopover facility if the transport cannot be completed, uninterrupted. Any stopover facility will have to be a rail siding or terminal area, and security arrangements should be approved in advance by the competent authority. During such stays the load carrying rail vehicle should be guarded or positioned in a secure locked and guarded rail yard, building or facility. NSS-13, 6.6)

6.2.2.3 Additional provisions for Category I nuclear material

When it is necessary to transport Category I nuclear material by rail it should be transported in a dedicated freight train, for which the nuclear material is its sole cargo. As far as operationally practicable, rail shipments should be uninterrupted, from origin to destination with any planned stops being limited to an absolute minimum and included in the TSP which is approved by the competent authority. During any stops extra vigilance should be maintained.

Load carrying rail vehicles should be specifically designed to resist attack by equipping them with technical measures to detect, deter, and delay access to the shipment. Accompanying guards should be (a) positioned to travel on the train close to the conveyance to have a proper effective surveillance and where best to respond to an attack, (b) should be capable of communicating with the train engineer, and (c) capable of initiating appropriate response.

Because of the need to prevent tampering and protect design information of the physical protection equipment, even when empty the rail carriage should be protected from unauthorized access or observation.

6.2.3. Additional Provisions for Maritime Transport

Although there are no additional International Maritime Organization (IMO) physical protection regulations it can be noted that the IMO do have:
(a) International Ship and Port Facility Security Code and
(b) Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988
(c) International Convention for the Safety of Life at Sea (SOLAS 74 amended).

Which are both developed to protect Member States and shipping against the use of ships being used as weapons of mass destruction and the illegalization of the transport of nuclear materials out of the IAEA safeguards

Shippers should only consign nuclear material for maritime transport to ships flagged to States which have accepted responsibility for the security of the nuclear material as defined in the CPPNM.

6.2.3.1 Additional provisions for Category I and II nuclear material

When operationally practicable, transport on inland waterways should be avoided

Consideration should be given to (a) having guards accompany travel load-carrying ship; and (b) designing and equipping the container, compartment and/or ship to resist attack. Compliance to the International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High-Level Radioactive Wastes on Board Ships (INF Code) stipulated by the International Maritime Organization (IMO) can be considered to satisfy (b) above.

Packages of nuclear material should be situated within the ship such that they are protected by the design of the ship, so as to delay any attack. If the transport cannot be completed uninterrupted prior arrangements should be made for an appropriately equipped and secured maritime stopover facility. Security arrangements should be approved in advance by the competent authority for any stopover facility. During such stays the load carrying ship should be docked in a secure port facility. (NSS-13, 6.6)

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

6.2.3.2 Additional provisions for Category I nuclear material

Maritime transport of Category I nuclear material should be carried out on a dedicated ship. During Category I shipments, the only other acceptable cargo would be nuclear material. The ship should be specifically designed or modified to resist attack and to carry nuclear cargo. The nuclear material should be placed in a secure compartment or freight container which is locked and sealed. (NSS-13, 6.31, 6.42)
Security personnel should search:

— All personal items as they are brought on-board the ship.
— All persons entering the secure area
— All stores for the voyage as they are brought on to the ship.

Prior to commencing loading of the shipment areas including:

— Adjacent dockside areas
— Adjacent compartments
— The whole ship including stores and engine room
— Underwater section of the hull

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

Critically sensitive areas and systems such as engine room, navigation bridge, communications areas and guards positions should be secured with limited access and should be kept lock at all times during the transport. The ship should have a hardened control room for the purpose of command and control of the guards. The control room should be staffed by the guards’ command staff and, where possible, be in a location near the centre line of the ship with other compartments located round it to:

— Prevent disablement from outside ship attacks
— Delay any attack from within the ship

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

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

Ports of call along the route should be avoided
Because of the need to prevent tampering and protect design information of the physical protection equipment, even when empty the ship should be protected from unauthorised access or observation.

6.2.4. **Additional Provisions for Air Transport**

6.2.4.1 **Additional provisions for Category I, II and III nuclear material**

For air transport of nuclear material, shipment should be carried in accordance with the applicable security provisions (Annex 17 of the Convention on International Civil Aviation). Loading should be arranged, as far operational practicable, in such a way that the nuclear material doesn't need to be unloaded at stop-overs.

If the planned air transport cannot be completed, uninterrupted, or only with one aircraft then consideration should be given to making prior arrangement for storage of the consignment consistent with the category of the nuclear material. (NSS-13, 6.6)

6.2.4.2 **Additional provisions for Category I and II nuclear material**

Shipments of Category II should only be made in a cargo-only-aircraft in a secure compartment or container that is locked and sealed. (NSS-13, 6.31)

6.2.4.3 **Additional provisions for Category I nuclear material**

Shipments of Category I should only be transported by aircraft designated for cargo only and for which the nuclear material is its sole cargo. It is further recommended that air shipments of nuclear material be made in an aircraft whose flag country is a party to the Chicago Convention. (NSS-13, 6.43)

6.3. **ADDITIONAL PHYSICAL PROTECTION MEASURES BASED ON POTENTIAL RADIOLOGICAL CONSEQUENCES**

Some nuclear material in Category III or less than Category III should be subject to additional security requirements based on their potential radiological consequences if intentionally dispersed. The widespread dispersal of plutonium in Category III (< 500 grams) or less than Category III (less than 15 grams) could result in sufficiently high consequences that the level of protection given to prevent its acquisition for use in a nuclear explosive device is not as stringent as the level of protection that is appropriate to prevent its use in a radiological dispersal device. In these cases the materials should be categorized based on their radiological properties and the protection measures recommended in “Security in Transport of Radioactive Material” (NSS-9) should be applied in addition to the measures recommended in this publication. Section 4.2 provides guidance on the process that can be used to make this determination.
Based on its potential radiological consequences, some material below Category III may fall into the "basic security level" as defined in NSS-9. This would imply that in addition to prudent management practices the following physical protection measures should be applied, including:

- Basic security awareness training
- Personnel identity verification
- Security verification of conveyances
- Written instructions
- Exchange of security related information
- Trustworthiness determination

Similarly, some Category III material may have potential radiological consequences that place it in the "enhanced security level" and more stringent physical protection measures are recommended in NSS-14 and described in detail in NSS-9 than those contained in this publication. These measures include:

- Identification of carriers and shippers
- Security plans
- Advance notification
- Tracking devices
- Communications from the conveyance
- Additional security provisions for transport by road, rail and inland waterway

The physical protection measures required for the basic and enhanced security levels are fully described in NSS-9.
7. REQUIREMENTS FOR MEASURES TO LOCATE AND RECOVER NUCLEAR MATERIAL MISSING OR STOLEN DURING TRANSPORT

7.1. STATE RESPONSIBILITIES

The State's physical protection regime should include provisions for providing information and technical assistance in support of rapid and comprehensive measures for locating and recovering missing or stolen nuclear material. The State should ensure within its regulatory framework that shippers, carriers, and receivers are required to report lost, missing, or stolen nuclear materials. The roles and responsibilities for and recovery of nuclear materials should be clearly established (NSS-13, 3.9).

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

Where there is transboundary movement of nuclear materials, there should be appropriate coordination between the States and clear responsibilities for the location and recovery of nuclear materials out of regulatory control [NSS-15]. States should cooperate with each other in the location and recovery of lost or missing nuclear materials. Once the location of the material has been identified in a particular State, that State becomes the lead State in recovery and securing of the material. The tracking and prosecution procedures, if necessary, are to be co-ordinated between States.

When it has been reported to a State that nuclear material is missing or has been stolen, it is recommended the State informs bordering States of the event, so that they may alert the law enforcement organizations, and draw upon States assets with the capability of monitoring the presence of nuclear materials. However, it must be remembered there may be differences in States’ abilities to respond to lost or missing nuclear materials.

Once a package 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 15 ‘Nuclear Security Recommendations on Nuclear and Other Radioactive Materials out of Regulatory Control’, (NSS-15). In particular, the State should require that non-compliances are reported to all relevant competent authorities. When it has been reported to a State that nuclear material is missing or has been stolen, the State should notify relevant international organizations and other States in accordance with international obligations and national legislation.[NSS-15]

A State that has located and recovered nuclear material that has been reported lost or stolen from another State should safely and securely store the material and then, where appropriate, work with the State in which the control has been lost to arrange the safe and secure return of the material. Actions
taken by States holding the material should be consistent with national policies, procedures and with applicable bilateral and multilateral agreements [NSS-15].

The development of contingency plans for the location and recovery of nuclear material should be a joint effort between the State and the shipper/carerrier. The State’s regulatory framework should clearly specify the requirements for location and recovery actions and response capabilities that will be provided by the State, what are to be provided by the private sector, and how these are to be coordinated. In particular, the contingency plans should be harmonized with the national nuclear security response plan and the plans of the individual competent authorities responsible for implementing the national response plan for nuclear security.

The State should have clearly defined roles and responsibilities for the various organizations in its contingency plan. The latter should include rapid and comprehensive measures for the location and recovery of the missing nuclear material. Where various State organizations have differing contingency plans, they must all be coordinated together with the shipper’s/carerrier’s contingency plans. (NSS-13, 6.46)

Contingency plans for the location and recovery of lost nuclear material should be reviewed and if required updated on a regular basis. (NSS-13, 6.51)

The State should arrange regular exercises with the appropriate State entities to validate the contingency plans on the location and recovery of nuclear materials and train personnel in how to react in such a situation. (NSS-13, 6.51)

7.2. THE CARRIERS RESPONSIBILITIES

The carrier should be alert during transport for any indications that packages have been removed from the conveyance or tampered with and should verify during delivery that no packages are missing or have been tampered with. (NSS No13, 6.52)

Once a carrier suspects that a package has been lost or removed from a conveyance, it is a carrier’s responsibility to initiate an immediate search to ensure the packages have not been misplaced and are still under their control. As good practice the carrier may wish to notify the competent authority of when it suspects a package may be lost or removed. Once it has been verified a package is not under their control they should immediately notify the relevant authorities and the shipper. If packages are found to be still under the carrier’s control, the carrier should inform the relevant authorities and the shipper.

If it is discovered that a package has been tampered with during transport the carrier should notify the relevant authorities and shipper.
Once it has been determined that packages are lost, missing, have been stolen or have been tampered with, the carrier should assist the competent authority and State organizations in any way possible to locate the packages; for instance, tracing back previous movements and providing any requested information that could assist in identifying the missing package. Also, the carrier should cooperate during investigations and prosecutions. (NSS-13, 6.55)
8. MEASURES FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL AGAINST SABOTAGE DURING TRANSPORT

Protection against sabotage needs to be implemented with consideration to the measures for safety and against unauthorized removal. Careful consideration should be given to the impact of any changes to achieve sabotage resistance.

Most measures of physical protection described in section 6 of this publication contribute to protect a shipment against sabotage.

Physical protection measures that minimize success of sabotage acts can also enhance protection against unauthorised removal, but may complicate operational aspects of transport.

8.1. GENERAL APPROACH FOR DESIGNING MEASURES AGAINST SABOTAGE

8.1.1 Threat assessment and Design Basis Threat

The State should assess the known and postulated threats, related to nuclear material transport and ensure that the evaluation is adequate and maintained current. (NSS13 3.37) In this process for sabotage, attention should be paid to adversaries with the intent and capability to commit acts of sabotage. This may differ from adversaries with the intentions of unauthorized removal. In contrast to unauthorized removal where the goal is to gain control of material for illicit use, an act of sabotage against a nuclear material shipment is an act with a goal of inflicting actual radiological consequences on populations and to the environment. However, it has to be noticed that an act of sabotage needs not be successful (release material or cause radiological consequences) to achieve some aspects of those goals. (NSS13 3.34 and 3.37)

In the case where the State is issuing a DBT, the State may consider issuing a specific DBT related to sabotage. The DBT for sabotage may nevertheless be based on the same assumptions regarding means of potential opponents as is the DBT for theft and removal. The difference in the threat between theft or removal and sabotage essentially relies on the development of scenarios.

There are many potential sabotage modalities that could be considered and combined in the vulnerability assessment for an attack on nuclear 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.
8.1.2 Development of specific Threat scenarios

The 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 in getting access and control of the material while the second phase consists in the opponents escaping with the material after they have gained its control; in contrast, sabotage is limited to one phase: defeating the protection of the nuclear material by means of weapons or intrusive tools and create a radiological hazard to the population or to the environment.

Sabotage scenarios reflect the capability of the threat as determined by the State’s intelligence gathering capability. One aspect of a scenario is the number of persons that could be involved together with their training and experience. A second aspect is the attack methods or modalities they can bring to the scenario to achieve the sabotage objective. The objective is the release of radioactive material in sufficient quantity to produce serious radiological harm to individuals and populations which lead to significant socio-economic penalties on the State or the nuclear industry. However, it must be realized that a successful sabotage event, even one producing minimal radiological harm, will have serious impact on the credibility of the State’s ability to protect its citizens.

8.1.3 Target identification and ranking

From a State’s standpoint, potential targets for sabotage might be any nuclear material shipment occurring on the territory of the State or carried by a ship or aircraft flagged or registered to the State in international water or airspace. Nevertheless, the State should identify which shipments it believes warrant protection against sabotage due to the potential to cause unacceptable radiological consequences, and consider, in order to do so, following the principles introduced in section 4.3 of this publication.

With the objective of pre-estimating potential consequences associated with the sabotage of nuclear material shipments, attention needs to be paid to potential radiological consequences, mostly being reflected by the activity of the nuclides contained by the nuclear material, but also by its physical and chemical form. In a general manner, the nuclides contained in materials listed in Table 1 that may pose the greatest attractiveness for sabotage are those included in irradiated reactor fuel, and plutonium. Referring to safety considerations and to the Transport Regulations in particular, these nuclides present the most important radiological potential as their activity limitation for shipment in excepted packages, designated by $A_2$, is very low in comparison to others. As a consequence shipments of irradiated fuel or plutonium involve thousands to millions of $A_2$s, reflecting the important potential consequences that might result from the sabotage of such packages.

Other nuclear materials listed in Table 1 of section 4.1 have unlimited or relatively large $A_2$ values which means that shipments of even large mass or volume of the material might amount to relatively
few A2s. Even total release, which might be possible would produce limited radiological impact, but
economic and sociological impact.

However, some nuclear material with a subsidiary hazard e.g. uranium hexafluoride, may also present
severe chemical/toxic hazards. The appropriate competent authority should determine if such
materials warrant protection against sabotage.

8.1.4 Estimating the consequences of sabotage considering the threat and the targets: the
Vulnerability Assessment

The shipper/carrier should seek to minimize the success of an act of sabotage.

Considering the targets determined on the basis of the pre estimation described above and the threat
assessment, or if applicable the Design Basis Threat, the State or the competent authority should
consider obtaining a precise estimation of the consequences in terms of radiological consequences of
the Threat acting on the targets. This phase of estimation is currently considered as a vulnerability
assessment (see also ANNEX III).

In order to achieve a valid vulnerability assessment, both theoretical and numerical tools applicable to
determine weapons’ performance against packaging’s resistance will be useful. The best way to
ensure the validity of the assessment remains the use of specific experiments in which the actual
package is used as a target to the weapon considered to be representative of the Design Basis Threat
as defined by the Competent Authority with input from the State’s intelligence/defence organizations.
Frequently such specific information is not available and approximations and/or arguments from
similar cases are needed.

In assessing 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
nuclear material packaging will provide some protection for the nuclear material. The degree of
protection provided varies with the material being transported. Some nuclear materials, such as
irradiated nuclear fuel, require robust heavily shielded packages that provide substantial protection.
Other materials, such as uranium, do not require shielded packages and the protection provided by the
packaging will be minimal.

The vulnerability assessment needs to conclude whether the package safety provisions, such as its
shield walls and containment structure, as well as the protection measures against theft and removal
are sufficient in order to defeat the threat. If not sufficient, the vulnerability assessment needs to
conclude how important the damage caused to the package is and the likely release of radioactive
material (nature, mass and physical properties of the nuclides released). In addition, the vulnerability
assessment should consider whether the sabotage would result in an unacceptable radiological consequence (as defined by the State).

Such assessment might be more efficiently conducted by the shipper or the carrier with the support of laboratories specialized in the domain of weapons and armour testing, but, in the end, an assessment file should be produced for review by the Competent Authority as a basis for approval of the shipment and preparation of a shipment contingency plan.

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

- damage due to the blast of the explosive (generally limited to a few hundred meters)
- dispersion of large particles or pieces of nuclear material (generally limited to a few hundred meters)
- airborne dispersion of smaller particles including respirable particles (these can be carried thousands of meters depending on the buoyancy of the plume created by the blast, accompanying fires, etc.)

In the case where the vulnerability assessment shows that the package safety provisions and the protection measures against theft and removal are not sufficient in order to defeat the threat, the vulnerability assessment needs to determine the amount of radioactive material released, and the activity it represents including the amount released under respirable form. Subsequently, this amount of material released may be used as a source term for a dose calculation in the vicinity of the shipment considered as a target of the postulated act of sabotage.

For any radioactive material, including nuclear materials, the radiological consequences of sabotage that results in a release of the material include:

- direct radiation dose from unshielded material that is localized (like an unshielded special form source),
- direct radiation dose from widely dispersed material in inhabited areas that produces both a radiological and economic consequence,
- internal radiation dose from material that is inhaled during or shortly after a successful sabotage event, 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:
Package or shipment radionuclide content; and

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

### 8.1.5 Results and conclusion of the vulnerability assessment

Considering the release determined as a result of the vulnerability assessment, the activity released should be compared to the source term used in the construction of the nuclear material transport contingency plans.

If the released activity estimated is actually covered by the source term used in the definition of the current contingency plan, then it can be concluded that this plan and the protective measures outlined in the TSP is also well designed to handle a sabotage scenario; nevertheless specific considerations need to be taken into account by the response teams (see Section 9);

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

For effective planning in response to nuclear material sabotage situations (or any other nuclear or radiological emergency), it is important that there be a set of appropriate dose criteria at which protective and response actions will be taken immediately to avoid severe radiological effects.

The derived dose criteria, as they relate to the types and amounts of nuclear materials in transport, will be one of the principal determinants of the amount of effort taken to minimize the potential radiological impacts of a successful sabotage event on nuclear materials transport campaigns and in the adaptation of the shipment contingency plan to sabotage initiated situations.

The adaptation of the contingency plan based on the results presented by the carrier or the shipper and approved by the competent authority, should be undertaken by all entities which are part to the safety contingency plan design process.

Alternately, it may be possible to add some additional mitigating feature to the transport package or its conveyance, namely the physical protection measures against sabotage discussed below, to limit the projected release to an acceptable value.

### 8.2. DEFINING PHYSICAL PROTECTION MEASURES AGAINST SABOTAGE

The two following sections apply to the carrier and/or the shipper, who is in charge of implementing additional measures to protect nuclear material against sabotage.
8.2.1 Applicable Physical Protection Measures

There are a wide variety of materials and concepts that could be applied to existing packaging 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; providing a sufficient delay or even prevent access to the package, or preventing visual observation of the package. Also measures to reduce the effectiveness of explosives or to reduce penetration abilities could be considered.

Most of the measures will have impact on operation of the transport system because additional procedures will be required in preparing a shipment however the measures should not adversely affect the safety of the package.

8.2.2 Applicable Organizational Measures

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

Operational measures might include routing 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.
9. MEASURES TO MITIGATE OR MINIMIZE THE RADIOLOGICAL CONSEQUENCES OF SABOTAGE DURING TRANSPORT

In addition to a State being prepared to respond to an act or attempted act of unauthorized removal of nuclear material in transport, the State should also be prepared to respond to an act of sabotage. An act of sabotage may result in radiological consequences that need to be mitigated in order to minimize the impact on persons and the environment. Security for the shipment must be maintained during such a response and this requires careful planning and coordination between security and safety response forces. (NSS-13, 6.60)

The radiological consequences of an act of sabotage would be similar in many respects to a severe transport accident that results in a release of the radioactive contents of the packages. However, there also may be casualties from the act of sabotage and security of the site must be maintained for the protection of the cargo and preservation of evidence that may be required for criminal investigations.

Detailed guidance on planning and preparing for transport accidents is provided in an IAEA Safety Guide on Planning and Preparing for Emergency Response to Transport Accidents Involving Radioactive Material [9]. This publication provides guidance on specific measures to take in the event of a release of radioactive (including nuclear) material.

9.1. RESPONSIBILITIES

When an act of sabotage involving nuclear material occurs during transport several governmental organizations, the shipper, the carrier and guards/escort/security response personnel have responsibilities to act to mitigate its consequences. This response may consists of life saving, medical aid, fire suppression and control, securing the area to ensure the physical protection of the nuclear material and the police work associated with a subsequent investigation. In addition, consideration should be given to calling in specialized organizations trained to deal with radioactive material to assess the event and implement the protective measures used to contain, control or eliminate any radiological hazard. The degree of involvement of the various organizations may vary during the progress of the operation.

The responsibilities for planning and dealing with an act of sabotage are generally divided among several involved organizations and persons. The severity of the event and the category of the nuclear material involved (including the potential radiological consequences) generally determine the level of governmental response and involvement. Because the governmental responsibilities and responses are dependent on the legal framework of the State concerned, and therefore may vary among States, designation within a State of a ‘national coordinating authority’ to provide a focal point may be useful for developing and coordinating governmental response plans for sabotage involving nuclear material.
shipments. This may be useful for coordinating the development of national, provincial and local emergency response plans and facilitating proper emergency preparedness. The State should clearly define the roles and responsibilities of all governmental levels (local, provincial and national), shippers and carriers.

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

9.2. PLANNING

The State should establish a contingency plan which includes acts of sabotage during nuclear material transport. This overall plan should provide the basis for contingency plans prepared by shippers and/or carriers. The State should ensure that relevant entities conduct exercises to assess and validate the elements of the contingency plan related to acts of sabotage (NSS-13, 6.62, 6.63, 6.66 and 6.68).

The State contingency plan should reflect arrangements and protocols between State response organizations, carriers and other involved organizations (such as radiation and environment protection agencies) for coordination of measures to prevent further damage from dispersed nuclear material while at the same time securing the material and protecting emergency personnel. (NSS-13, 6.65)

The State should develop and provide guidance for personnel that might be involved in response to an act of sabotage with radiological consequences, for example, for police or fire personnel that should be aware of basic radiation protection measures and actions. Such guidance could build on existing guidance that covers procedures and measures to be taken in the event of a transport accident that involves possible radioactive material release.

9.3. CARRIER ACTIONS

The carrier should ensure that its personnel are fully trained and prepared to act in full coordination with guards, response forces and law enforcement agencies in the event of an act of sabotage or other activation of the contingency plan (NSS-13, 6.70).

In the event of an act of sabotage Carrier or other designated personnel accompanying the shipment should immediately initiate the actions required in the contingency plan. The carrier or other designated personnel should also notify the transport control centre or the carrier management as specified in the contingency plan. (NSS-13, 6.72)
Immediately following any act of sabotage the carrier or other designated personnel and/or guards should take measures to secure the nuclear material, the incident site and the conveyance. Measures to minimize the radiological consequences of the act should also be taken as specified in the contingency plan. (NSS-13, 6.73)
REFERENCES


ANNEX I. THE TRANSPORT SECURITY PLAN

An example structure of the Transport Security Plan (TSP) when the performance-based method is applied is shown in the figure below. While a State may need to modify this outline, it contains all the information that the State needs to monitor the transport activities of those who need to transport nuclear materials. States should require this structure or a structure similar to this to facilitate understanding between shippers, carriers, receivers and regulators both domestically and internationally.

Figure. Example Structure of the Transport Security Plan for the Performance-based Method.

1. Administrative Requirements/Information
   1.1 Allocation of Responsibilities
   1.2 Policies and Operational Procedures
      1.2.1 Vulnerability Assessment
      1.2.2 Testing and Evaluation of the Security Plan
      1.2.3 Review and Update of the Security Plan
      1.2.4 Response to Higher Threat Conditions
      1.2.5 Reporting of Threats or Incidents
   1.3 Training Requirements
   1.4 Information Management
      1.4.1 Records Retention
      1.4.2 Confidentiality and Protection of Information
   1.5 Trustworthiness of Personnel

2. Shipment Security
   2.1 Nuclear Material to be Transported
   2.2 Description of the Security System
      2.2.1 Packages and Conveyances
      2.2.2 Planned and Alternate Routes and Modes of Transport
      2.2.3 Physical protection measures
      2.2.4 Communications and Positional Tracking for Normal Operations
In addition, since the performance-based method necessitates that the entity responsible for preparing/submitting the TSP, have access to knowledge emanating from the State’s threat assessments or DBT, enhanced confidentiality and protection of the information in the TSP, or separate elements thereof may be required, allowing wider distribution of some elements.

For the prescriptive method, the listing of provisions required by the competent authority should be inserted in Section AI 2.2.

The following sections outline the recommended details that should be considered for inclusion in a TSP for a shipment undertaken following the performance-based method. In the event that the entity responsible for preparing/submitting the TSP is required by the competent authority to apply the performance-based or combined method, a vulnerability assessment may or may not be required, see Annex III.

AI.1. ADMINISTRATIVE REQUIREMENTS/INFORMATION

The Administrative Requirements and Administrative section should include information on the complete legal name and address of the entity responsible for preparing/submitting the TSP, plus all appropriate phone, fax, and e-mail addresses of those who are applying for approval of the TSP. This should include information about the shipper, carriers or others who might be involved with the proposed shipment, including guards employed for the shipment, and information about the receiver and transit States when international shipments are contemplated. It should also contain detailed information in subsections as elaborated below.

AI.1.1. Allocation of Responsibilities

The TSP should clearly establish responsibility for, and ownership of, the security plan and all provisions and measures specified therein. It should also identify all involved personnel that have the appropriate authority to carry out their responsibilities, and should include the shipper, carrier or receiver having direct responsibility for the security of the nuclear material in any particular mode or phase of the transport.

In the event that any transport activities are subcontracted, the TSP should identify all contractual arrangements that will be required to develop and comply with the security plan. Also, whenever responsibility for a shipment is to be changed from one party to another (e.g. between carriers at a national border, or between a carrier or receiver, or a facility operator when the shipment is being placed into in-transit storage), the transfer of responsibilities should be specified.
AI.1.2. Policies and Operational Procedures

Clear statements of policies and operational procedures should be documented in this section of the TSP, including measures that detail policies (e.g., policies on response procedures to higher threat conditions, new employee/employment verification), operating practices (e.g. choice/use of routes where known, use of guards, access to nuclear material packages at en route temporary storage facilities, and limiting proximity to potentially vulnerable infrastructure), and equipment and resources that are to be used to reduce security risk.

1.2.1 Vulnerability Assessment

For the performance-based method, and options of the combined method, the administrative and technical requirements specified in the State’s regulatory framework should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment. The competent authority may require the entity responsible for preparing/submitting the TSP to prepare a vulnerability assessment, see Annex III.

1.2.2 Testing and evaluation of the TSP

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

1.2.3 Review and update of the TSP

TSPs should be reviewed periodically to ensure that the latest information available to the State relative to security of nuclear material shipments is taken into account. Because the TSP should be reviewed periodically, it should specify when and how the reviews and updates are to be accomplished.

1.2.4 Response to higher threat conditions

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

1.2.5 Reporting of threats or incidents

The TSP should require that any incidents or unscheduled delays that occur during transport be documented by the carrier and reported to the shipper, receiver and if applicable the competent authority. The TSP should also specify that a review of physical protection arrangements be undertaken after a shipment is completed in order to evaluate the effectiveness of the TSP and to identify any necessary improvements which may be made to optimize its effectiveness for future shipments.
AI.1.3. Training Requirements

This section of the TSP should identify the training that will be conducted and the exercises that will be arranged, and specify the schedule that will be followed for each since the State competent authority or equivalent body may wish to witness the exercises. The training and exercises should be directed toward all appropriate aspects of physical protection, including those for organizational interfaces and specified functions required to be performed for emergency response. Arrangements should be made for the results of exercises to be systematically evaluated and, as appropriate, to be evaluated by the appropriate State regulatory body. The results of all training exercises should be documented, and any corrective actions identified during the process should be expeditiously implemented.

AI.1.4. Information Management

The TSP should clearly define the actions and any measures that will be taken in order to maintain confidentially of information deemed sensitive or classified by the competent authority. Information management procedures should also ensure that the distribution of sensitive transport information is limited to appropriate individuals on a need-to-know basis. Such measures should not preclude the proper application of provisions needed in transport documents and shippers declaration as required by the transport safety Regulations [6].

1.4.1 Records retention

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

1.4.2 Confidentiality and protection of information

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

Since a TSP describes the transport of Category I, II or III nuclear material it will contain sensitive information on aspects of the shipment including details on the package and the load conveyance used
to transport the material. Thus, the TSP should be handled in such a way as to protect such
information in accordance with the applicable provisions of the State and other appropriate
documents. The entity responsible for preparing/submitting the TSP should follow the provisions
determined by the State, taking all necessary precautions to prevent unauthorized access to any
sensitive information contained in the TSP. These precautions should be defined in the TSP.

AI.1.5. Trustworthiness of Personnel

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

AI.2. SHIPMENT SECURITY

Operating practices should also identify equipment and resources that are to be used to reduce security
risks. In addition Operating practices should be described in the TSP.

— choice/use of routes where known including identification of safe havens;
— use of guards;
— engineered systems to be used to enhance security;
— limiting access to nuclear material packages needing the enhanced security level in temporary
  storage while en route; and
— special actions relative to transport in close proximity to potentially vulnerable infrastructure.

These practices should include a general discussion of these practices, the TSP should contain specific
subsections as follows

AI.2.1. Description of the Nuclear Material to be Transported

This section of the TSP should include information on the name of the nuclear material (i.e.
plutonium, U-233, U-235, or, irradiated fuel), its category (i.e. Category I, II, or III), quantity of the
nuclear material, form of the material, chemical and physical characteristics of the material, isotopic
composition of the material, enrichment values, radiation levels, and any other applicable data (e.g.
age and burn-up of irradiated fuels).
AI.2.2. Description of the Security System

This section of the TSP should address the manner in which all of the elements that constitute the transport physical protection system are designed and maintained.

2.2.1 Packages and conveyances

This section of the TSP should identify packages to be used and any information of these designs pertinent to security. If specially designed conveyances are to be used, they should be described along with any protective capabilities those conveyances might provide (i.e. deterrence, detection or delay).

2.2.2 Planned and alternate routes and modes of transport

This section of the TSP should contain a detailed description of the planned modes of transport and the planned primary routes to be followed and all available information on these routes that would be useful to the concerned State Authorities, competent authority, carrier personnel, and guard and response forces should be discussed.

That information should include, as applicable, current applicable road, rail, inland waterway, port facility, transfer and stopover facility, border crossing and airport conditions that affect the transport, including:

- items such as allowable speeds;
- areas where repair or construction work is being, or is expected to be, performed;
- potential impacts of weather conditions;
- planned transfer point and stopover facility capabilities;
- refuelling sites; and
- safe havens and subsistence locations.

Alternate routes that could be used in case of emergency should also be defined and discussed including expected conditions on those routes and information similar to that reported on the proposed primary routes.

2.2.3 Physical protection measures

This section of the TSP should address how the shipper has designed its transport physical protection system to accomplish the multiple security objectives of deterrence, detection, assessment, delay, and response. This section of the TSP should present physical protection measures that are proposed recognizing that, in many ways security during the transport of nuclear materials is more challenging than security at a nuclear facility. It is extremely difficult, if not impossible, to limit public access to shipments being made in public areas. Also, it should be recognized that unauthorized removal, sabotage and other security incidents can occur anywhere along a transport route, which may extend
over a significant distance and in areas of minimal population density, thereby giving an adversary a
wide choice of potential attack locations. This choice could be at locations where it will be extremely
difficult for any sizeable response force to arrive within a useful period of time; in which case an
alternate response force would need to follow the transport convoy at a reasonable distance.

2.2.4 Communication and positional tracking for normal operations
This section of the TSP should discuss the structure of the entire primary and alternate
communications system for the proposed transport operation. Any system proposed to be used for
tracking the conveyances should be described; and they should be located at, and operated by a
transport control centre or an alternative central point of communication if one is required by the
competent authority. Alternate communications systems, when required, should not be vulnerable to
the same failure mode as the primary system in order to ensure at least one means of communication
is available at all times.

2.2.5 Command and control for normal operations
This section of the TSP should discuss command and control procedures and establishment of persons
of authority for each phase of the transport operation. It should address the entire command and
control arrangement for the shipment and define how it meshes with the communications structure
and procedures. It should discuss command and control procedures, designating the responsible
authority and appropriate chain of command for each phase of the transport operation, making clear
who has authority to make critical decisions for each phase of the transport operation for routine
situations, or a response to an emergency or security event. When guards are used, the TSP should
also define command and co-ordination procedures between the response force and the guards, and
between the primary response force and any secondary response forces that may be planned for
deployment.

The chain of command should be defined clearly and simply, and should also define who has the
authority to give the final decision to start, delay, cancel or interrupt the transport operation, and to
take action in the event of an emergency or security event. It should specifically define the roles and
responsibilities of the transport commander, the response force commander, and the transport control
centre; and should elaborate on how and when handoff of command and control would be made from
the transport commander to the response force commander in the event this becomes necessary.

A1.2.3. Maintenance and Testing of Systems and Equipment
This section of the TSP should address the manner in which all of the systems involved in the
shipment(s) are designed and maintained.

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 operations in order to ensure the secure transport of
the involved nuclear materials. Categories of equipment that should be inspected and tested before
the commencement of a transportation operation include:

— all transport conveyances;
— communications equipment and tracking systems;
— any delay systems (e.g. personnel barriers, vehicle immobilization systems) built into the
  transport packages or conveyances; and
— individual guards and response force weapons and tactical equipment, protective gear and
  communication devices.

AI.2.4. Pre-Shipment Checks
This section of the TSP should address the competent authority requirements and the shipper or
carrier arrangements for pre-shipment checks or readiness reviews.

AI.3. RESPONSE PLANNING

AI.3.1. Emergency Arrangements
This section of the TSP should address planned actions and procedures in the event of an emergency
situation such as a road closure, vehicle breakdown, vehicle accident, or driver illness that may occur
during the shipment. Emergency arrangements include but are not limited to: backup vehicle and
driver, heavy towing and lifting capability, safe havens, and alternative routes.

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

AI.3.2. Contingency Plans
The security plan should nominate specific people who have the responsibility and authority to
execute contingency plans should a security event occur.

This section should also address the capability to ensure that any transport control centre or alternative
central point of communication that is used can be made immediately aware a security event and the
time and place that it was initiated. It should also address planned actions and procedures necessary
to be taken by the control centre or alternative central point of communication should a security event
occur.
Appropriate protective measures and procedures should be employed in such a way that there is depth to the defences used during the shipment where, for example, the employment of guard and response forces are planned to facilitate establishing the defensive depth. It should therefore identify:

— any designated guards that are to accompany the shipment;
— all designated response force units/organizations that are assigned responsibilities for the shipment;
— any other State assets that are projected to be available to support the movement or assist in response to an incident or emergency; and
— all other support personnel, including fire, rescue and other asset units along the route, as applicable and the communications system required for appropriate information transfer.

3.2.1 Guards

A graded approach should be used in specifying plans for the guards in the TSP. For example, the competent authority may consider the use of guards accompanying shipments of Category III nuclear material; whereas it should require guard personnel to accompany Category I and II nuclear material shipments. If guards do not accompany the shipment, then the driver or operator of the conveyance, or another designated crew member, should be capable of providing surveillance of the material and all required notifications of adverse actions in accordance with information provided in the shipper or carriers TSP.

3.2.2 Response force

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

A1.3.3 Incident Communications, Command and Control

This section of the TSP should discuss the structure of the entire primary and alternate communications system for the proposed transport operation. Any system proposed to be used for tracking the conveyances should be described; and they should be located at, and operated by a transport control centre or an alternative central point of communication if one is required by the competent authority.
ANNEX II. THE VULNERABILITY ASSESSMENT

For the performance-based method, and options of the combined method, the administrative and technical requirements specified in the State’s regulatory framework should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment.

If required by the State, the TSP should specify that review of current or proposed operations and assessment of vulnerability will be carried out as appropriate, and that the resulting vulnerability assessment will be appropriately documented and utilized by the shipper or responsible authority in developing its physical protection measures that are required by the performance-based or method, or if required, the combined method.

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

The assessment of any security system performance requires a methodical approach in which the ability of the system to meet stated requirements is determined. Without this kind of approach, physical protection will only be based, at best, on conformance to feature-based (e.g. locks, access control, visual monitoring) or list-based requirements that may or may not provide anything other than perceived security risk reductions.

The vulnerability assessment process comprises three major phases:

— planning;
— conduct; and
— closure.

AII.1 PLANNING THE VULNERABILITY ASSESSMENT

A realistic evaluation of potential threats and their capabilities is an important aspect in undertaking a vulnerability assessment. In most cases, a vulnerability assessment is a sufficiently complex process that some reasonable amount of planning will help ensure that only work essential to the assessment is conducted and that the intended objectives are met. The amount of time spent depends on the size and complexity of the assessment. The planning phase includes the following activities:
AII.1.1 Establish the scope and objectives of the vulnerability assessment

In the initial planning phase it is necessary to determine the scope and objectives of the vulnerability assessment. The scope should include terms of reference including reference to relevant threat assessments and/DBT and any constraints.

The scope of work should also clearly define all expected deliverables and the complexity and rigor with which the assessment should be conducted. The complexity and rigor of the assessment will depend on:

— the nature of the shipment including the attractiveness of the material;
— the threat environment at the proposed time of shipment; and
— the time available to complete the assessment.

In transport, vulnerability may change dramatically during different stages of the transport operation, for different modes of transport and for different or alternative routes.

AII.1.2 Select knowledgeable team members, and define roles and responsibilities

With regards to sensitive information on type, category and quantity of nuclear materials to be transported, a team of experts may be created to ensure that a complete and accurate vulnerability assessment is produced. The team should include security specialists who can ensure that the vulnerability assessment is correct. The members of the team should have knowledge of security systems, response actions, data analysis, radioactive contamination, etc.

AII. 1.3 Develop a schedule with deliverables and resource requirements

Projects seldom go precisely to plan; when developing the schedule, thought must be given to realistic start and finish times and any foreseeable risks of not achieving all deliverables. All team members should be consulted to determine resources required to deliver the required outcomes in the allotted time.

AII.2 CONDUCTING THE VULNERABILITY ASSESSMENT

The process steps within the second phase of a vulnerability assessment are to:

— state the objectives of the security system
— describe the components of the security system;
— characterize the components of the security system; and
— analyse the ability of the system to meet the objectives.
AII.2.1 State the objectives of the security system

The vulnerability assessment starts with a statement of the objectives of the security system as provided by the competent authority. This section could usefully include the relevant aspects of the DBT or Threat Assessment.

AII.2.1 Describe the components of the security system

The tasks to be completed during this step of a vulnerability assessment includes a description of the components of the security system, the transportation system, the target (nuclear material), and where applicable, the response force.

A description of the Transportation system is important for establishing operational, safety, and physical constraints on the security system, as well as mode-specific requirements. Understanding the material being transported is important for establishing both feature-based requirements (e.g., a graded approach) and performance requirements (preferably established by a separate consequence-based risk analysis). The description of the response force includes information on weapons, tactics and training.

This section should include applicable information on all phases of the proposed shipment, such as any potential intermodal transfer operations, temporary transit (i.e. in transit) storage activities, routes that pass through both high-density and low-density population areas, etc.

AII.2.2 Characterize the components of the Security System

Characterization of a security system involves gathering data, and often includes the development and validation of models, to determine how the personnel, procedural, and technological elements of a security system perform in the face of attack as postulated by the DBT or the threat assessment. In general, these elements are evaluated in terms the ability to defeat the adversary, as deterrence has proven difficult to quantify. Note that defeat is almost always decomposed into the security functions detect, assess, delay, and respond (or response). Note also that the measures used to characterize security function performance should support the input requirements of the analysis techniques used in the following performance determination step. The performance data are gathered by conducting tests at the component and element level.

AII.2.3 Analyse the ability of the system to meet the objectives

The fourth step of the vulnerability assessment is to determine the performance of the security system in meeting the security objectives in relation to the threat. System models may be used and may be predictive (simulation) or schematic in nature, and range from the qualitative to quantitative in nature. The goal of using such models is to conduct an analysis to predict how the security system, as
currently operating or proposed, will perform against the DBT. System models, or at least particular
scenarios, may be validated through appropriate exercises, such as table top exercises, simulations and
force-on-force exercises.

AII.3 CLOSURE OF THE VULNERABILITY ASSESSMENT

The last phase of a vulnerability assessment has the goal of providing an accurate record of the
project. This should include such things as the methodology used, the assumptions made, the data
collected, and the effectiveness results. The manner and media used in reporting the results should be
usable to the ultimate customer that is tasked to make decisions regarding the adequacy of the security
system evaluated. The reporting of results is typically conducted by two methods: (a) briefings, and
(b) written reports.

In the event that the vulnerability assessment team concludes that the security system does not meet
the established objectives, the documentation should include recommendations concerning potential
solutions. Such solutions should be based on insights gained during the conduct of the vulnerability
assessment and not on a detailed assessment of various design options. While the personnel on a
vulnerability assessment team may be given responsibility for developing design recommendations in
addition to conducting the vulnerability assessment itself, this is properly considered a design upgrade
activity and not an assessment of an existing security system. On review of the results, the competent
authority and transport system owners or operators may also have the option to consider improving
the scope, resolution, or accuracy of the assessment in order to address apparent disparities between
security system requirements and performance projections. Because performance requirements are
often based on supporting risk assessments, changes in the material being transported (e.g., quantity)
will alter theft or sabotage consequences, and thus can alter the conclusions drawn.

If the competent authority feels that the State’s Requirements are not met by the vulnerability
assessment or the assessment is inadequate, it should be returned to the originator for additional
information and action.

{Some of the material in this Annex is adapted from “The Design and Evaluation of Physical
Protection Systems.” By Mary Lynn Garcia, Sandia National laboratories} to be checked (may be
from “Vulnerability Assessments of Physical Protection System” by same author)
DEFINITIONS

access delay. The element of a physical protection system designed to increase adversary penetration
time for entry into and/or exit from the nuclear facility or transport.

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

competent authority. Governmental organization(s) or institution(s) that has(have) been designated
by a State to carry out one or more nuclear security functions.

contingency plan. Predefined sets of actions for response to unauthorized acts indicative of attempted
unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

conveyance. For transport (a) by road or rail: any vehicle used for carriage of nuclear material cargo;
(b) by water: any seagoing ship or inland waterway craft, or any hold, compartment, or defined deck
area of a seagoing ship or inland waterway craft used for carriage of nuclear material cargo; and (c)
by air: any aircraft used for carriage of nuclear material cargo.

defence in depth. The combination of multiple layers of systems and measures that have to be
overcome or circumvented before physical protection is compromised.

design basis threat. The attributes and characteristics of potential insider and/or external adversaries,
who might attempt unauthorized removal or sabotage, against which a physical protection system is
designed and evaluated.

detection. The term “detection is defined in NSS-13 as “A process in a physical protection system
that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed
with the assessment of the cause of the alarm”.

For the detection of criminal or unauthorized acts with nuclear security implications, the term
“detection” is defined in NSS-15 as “Awareness of criminal act(s) or unauthorized act(s) with nuclear
security implications or measurements(s) indicating the unauthorized presence of nuclear material, or
other radioactive material at an associated facility or associated activity or a strategic location”.

force-on-force exercise. A performance test of the physical protection system that uses designated
trained personnel in the role of an adversary force to simulate an attack consistent with the threat or
the design basis threat.
**graded approach.** The application of physical protection measures proportional to the potential consequences of a malicious act.

**guard.** A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.

**insider.** One or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so.

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

**nuclear facility.** A facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of and for which a specific licence is required.

**nuclear material.** Material listed in Table 1, in Section 4 of this publication, including the material listed in its footnotes.

**nuclear security culture.** The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serves as means to support, enhance and sustain nuclear security.

**nuclear security event.** The term “nuclear security event” is defined in NSS-Fundamentals as “An event that has the potential or actual implications for nuclear security that must be addressed. The definition in NSS-13 is: “An event that is assessed as having implications for physical protection”.

**operator.** The term “operator” is defined in NSS-Fundamentals as “Any person, organization, or government entity licensed or authorized to undertake the operation of an associated facility or to perform an associated activity”. The definition in NSS-13 is: “Any person, organization, or government entity licensed or authorized to undertake the operation of a nuclear facility.

**performance testing.** Testing of the physical protection measures and the physical protection system to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements.

**physical barrier.** A fence, wall or similar impediment which provides access delay and complements access control.

**physical protection measures.** The personnel, procedures, and equipment that constitute a physical protection system.

**physical protection regime.** A State’s regime including:
— The legislative and regulatory framework governing the physical protection of nuclear material and nuclear facilities;
— The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;
— Facility and transport physical protection systems.

**physical protection system.** An integrated set of physical protection measures intended to prevent the completion of a malicious act.

**protected area.** Area inside a limited access area containing Category I or II nuclear material and/or sabotage targets surrounded by a physical barrier with additional physical protection measures.

**response forces.** Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorized removal or an act of sabotage.

**sabotage.** Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.

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

**shipment.** Specific movement of consignment (Nuclear Material) from origin to destination

**source term.** The type and amount of radioactive or hazardous material released to the environment following an incident. This is taken as an input for a dispersal and dose rate calculation.

**stand-off attack.** An attack, executed at a distance from the target nuclear facility or transport, which does not require adversary hands-on access to the target, or require the adversary to overcome the physical protection system.

**threat.** A person or group of persons with motivation, intention and capability to commit a malicious act.

**threat assessment.** An evaluation of the threats — based on available intelligence, law enforcement, and open source information — that describes the motivations, intentions, and capabilities of these threats.

**transport.** International or domestic carriage of nuclear material by any means of transportation, beginning with the departure from a nuclear facility of the shipper and ending with the arrival at a nuclear facility of the receiver.
transport control centre. A facility which provides for the continuous monitoring of a transport conveyance location and security status and for communication with the transport conveyance, shipper/receiver, carrier and, when appropriate, its guards and the response forces.

two person rule. A procedure that requires at least two authorized and knowledgeable persons to be present to verify that activities involving nuclear material and nuclear facilities are authorized to detect access or actions that are unauthorized.

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

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