CONTENTS

1. INTRODUCTION
   1.1. Background
   1.2. Purpose
   1.3. Scope
   1.4. Structure

2. DEFINITIONS

3. OBJECTIVES OF A STATE'S PHYSICAL PROTECTION REGIME

4. ELEMENTS OF A STATE'S PHYSICAL PROTECTION REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES
   4.1. State responsibility
   4.2. International transport
   4.3. Assignment of physical protection responsibilities
   4.4. Legislative and regulatory framework
   4.5. International cooperation and assistance
   4.6. Identification and assessment of threats
   4.7. Risk-based physical protection systems and measures
   4.8. Sustaining the physical protection regime
   4.9. Planning and preparedness for and response to nuclear security events

5. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE
   5.1. General
   5.2. Requirements for physical protection against unauthorized removal of nuclear material in use and storage
   5.3. Requirements for measures to locate and recover missing or stolen nuclear material

6. REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR FACILITIES AND NUCLEAR MATERIAL IN USE AND STORAGE
   6.1. General
   6.2. Basis for graded approach for physical protection against sabotage
   6.3. Requirements for process to design physical protection systems against sabotage
   6.4. Requirements for physical protection against sabotage at nuclear facilities
   6.5. Requirements for associated measures to mitigate and minimize the consequences of sabotage

7. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT
   7.1. Requirements for physical protection of nuclear material against unauthorized removal during transport
   7.2. Requirements for measures to locate and recover nuclear material missing or stolen during transport
   7.3. Requirements for physical protection of nuclear material against sabotage during transport
7.4. Requirements for associated measures to mitigate and minimize the radiological consequences of sabotage during transport

REFERENCES
1. INTRODUCTION

1.1. Background

1.1.1. The IAEA has established a nuclear security programme and instituted a Nuclear Security Series of publications to provide recommendations and guidance that States can use in establishing, implementing and maintaining a nuclear security regime.


1.1.4. The second tier set of Recommendations documents elaborates on the essential elements of nuclear security and presents the recommended requirements that should be implemented by States for the application of the fundamental principles.

1.1.5. The third and fourth tiers of Implementing Guides and Technical Guidance provide more detailed information on how to implement the recommendations using appropriate measures.

1.1.6. This recommendations document is complementary to the following two Nuclear Security Recommendations documents on:

• Radioactive Material and Associated Facilities [3], and
• Nuclear and Other Radioactive Material Out of Regulatory Control [4].

1.1.7. This publication is a recommendations document for the physical protection of nuclear material and nuclear facilities. It is also revision 5 of the INFCIRC/225 [5].

1.1.8. The Member States should use this publication to implement a comprehensive physical protection regime including any obligations and commitments they might have as parties to international instruments [6] related to the physical protection of nuclear material, especially the Amendment to the Convention on the Physical Protection of Nuclear Material of July 2005 [7].

1.2. Purpose

1.2.1. This publication provides a set of recommended requirements to achieve the four Physical Protection Objectives (see Section 3) and to apply the twelve Fundamental Principles (see Section 4) that were endorsed by the IAEA Board of Governors and General Conference in September 2001 [8].

1.2.2. The purpose of this publication is to provide guidance to States and competent authorities on how to develop or enhance, implement and maintain a physical protection regime for nuclear material and nuclear facilities, through establishment or improvement of their capabilities to implement legislative and regulatory programmes to address the protection of nuclear material and nuclear facilities in order to reduce the likelihood of malicious acts involving that material.

1.2.3. These recommended requirements are provided for consideration by States and competent authorities but are not mandatory upon a State and do not infringe on the sovereign rights of States.

1.3. Scope

1.3.1. This publication applies to the physical protection of nuclear material, including its physical protection during transport, and of nuclear facilities for the prevention of malicious acts intended to cause harmful radiological consequences.

---

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 also Revision 5 of INFCIRC/225, the term physical protection continues to be used throughout the publication.
1.3.2. Three types of risk should be taken into consideration for the protection of nuclear material and nuclear facilities:

- risk of unauthorized removal with the intent to construct a nuclear explosive device,
- risk of unauthorized removal with the intent of subsequent dispersal,
- risk of sabotage.

1.3.3. Protection requirements against unauthorized removal of nuclear material for potential subsequent offsite radiological dispersal are provided in Nuclear Security Recommendations on Radioactive Material and Associated facilities [3].

1.3.4. Nuclear material which is out of regulatory control is addressed in Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control [4]. That publication includes actions undertaken to locate and recover material after the reporting of lost, missing or stolen nuclear material to a competent authority (e.g. regulatory body or law enforcement authority) according to national regulation.

1.3.5. When a facility contains nuclear material and other radioactive material, the two sets of regulatory requirements should be considered and implemented in a manner that the more stringent requirements for physical protection are applied. This also applies to transport of nuclear material.

1.3.6. This publication does not provide safety requirements. Safety requirements are contained in the Safety Standards. However, the publication takes safety considerations into account.

1.3.7. This publication is intended for use in the physical protection of nuclear material and nuclear facilities used for civil purposes. Member States may decide whether on not to extend the publication’s use to other purposes.

1.4. Structure

1.4.1. Chapter 2 defines terms used in the publication. Italicized words in the text represent defined terms.

1.4.2. Chapter 3 provides objectives of a State’s physical protection regime for nuclear material and nuclear facilities.

1.4.3. Chapter 4 provides elements of a State’s physical protection regime for nuclear material and nuclear facilities.

1.4.4. Chapter 5 provides requirements for measures against unauthorized removal of nuclear material in use and storage.

1.4.5. Chapter 6 provides requirements for measures against sabotage of nuclear facilities and nuclear material in use and storage.

1.4.6. Chapter 7 provides requirements for measures against unauthorized removal and sabotage of nuclear material during transport.
2. DEFINITIONS

Definitions of terms used in the publication are listed below and are italicized in the text. These definitions are also listed in the Nuclear Security Glossary [1].

2.1. 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. Access delay can be accomplished by physical barriers, activated delays, and/or personnel.

2.2. CENTRAL ALARM STATION: An installation which provides for the complete and continuous alarm monitoring, assessment and communication with guards, facility management and response forces.

2.3. COMPETENT AUTHORITY: A governmental organization or institution that has been designated by a State to carry out one or more nuclear security functions.

2.4. CONTINGENCY PLAN: A predefined set of actions for responses to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

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

2.6. DEFENCE IN DEPTH: The combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised.

2.7. DESIGN BASIS THREAT: The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

2.8. DETECTION: 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.

2.9. FORCE-ON-FORCE EXERCISE: A performance test of the physical protection system that uses designated personnel in the role of an adversary force to simulate an attack consistent with the threat or the design basis threat.

2.10. GRADED APPROACH: The application of physical protection measures proportional to the potential consequences of a malicious act.

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

2.12. INNER AREA: An area with additional protection measures inside a protected area, where Category I nuclear material is used and/or stored.

2.13. 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.

2.14. LIMITED ACCESS AREA: Designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes.

2.15. MALICIOUS ACT: An act or attempt of unauthorized removal of nuclear material or sabotage.

2.16. 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 license is required.

2.17. NUCLEAR MATERIAL: Material listed in the “Table: Categorization of Nuclear Material” contained in Chapter 5, including the material listed in its footnotes.

2.18. NUCLEAR SECURITY CULTURE: The assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serves as a sustainable means to support and enhance nuclear security.

2.19. NUCLEAR SECURITY EVENT: An event that is assessed as having implications for physical protection.
2.20. OPERATOR: Any person, organization, or government entity licensed or authorized to undertake the operation of a nuclear facility.

2.21. PERFORMANCE TESTING: Testing of the physical protection system element(s) and the total 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.

2.22. PHYSICAL BARRIER: A fence, wall or similar impediment which provides access delay and complements access control.

2.23. PHYSICAL PROTECTION MEASURES: The personnel, procedures, and equipment that constitute a physical protection system.

2.24. 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 the implementation of the legislative and regulatory framework; and
- facility-level and activity-level physical protection systems.

2.25. PHYSICAL PROTECTION SYSTEM: An integrated set of physical protection measures intended to prevent the completion of a malicious act.

2.26. 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.

2.27. RESPONSE FORCES: Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage.

2.28. 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.

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

2.30. STAND-OFF ATTACK: An attack, executed at a distance from the target facility or transport, which does not require adversary hands-on access to the target, or require the adversary to overcome the physical protection system.

2.31. SUSTAINABILITY: The continuous capability of a State’s physical protection regime, together with the operator’s physical protection system at a nuclear facility and/or a carrier’s physical protection system during transport, of satisfying all performance and prescriptive requirements.

2.32. SYSTEM FOR NUCLEAR MATERIAL ACCOUNTANCY AND CONTROL: An integrated set of measures designed to provide information on, control of, and assurance of the presence of nuclear material, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures.

2.33. THREAT: A person or group of persons with motivation, intention and capability to commit a malicious act.

2.34. 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.

2.35. TRANSPORT: International or domestic carriage of nuclear material by any means of transportation, beginning with the departure from a facility of the shipper and ending with the arrival at a facility of the receiver.

2.36. 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.
2.37. 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 in order to detect access or actions that are unauthorized.

2.38. UNACCEPTABLE RADIOLOGICAL CONSEQUENCES: A level of radiological consequences, established by the State, above which the implementation of physical protection measures is warranted.

2.39. UNAUTHORIZED REMOVAL: The theft or other unlawful taking of nuclear material.

2.40. VITAL AREA: Area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences.
3. OBJECTIVES OF A STATE’S PHYSICAL PROTECTION REGIME

3.1. 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 sabotage**: mitigating or minimizing the radiological consequences of sabotage.

3.2. 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; and
- Mitigation of the consequences of a malicious act.

3.3. The objectives mentioned above should be addressed in an integrated and coordinated manner taking into account the different risks covered by nuclear security.
4. ELEMENTS OF A STATE’S PHYSICAL PROTECTION REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES

4.1. State responsibility

The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State. (FUNDAMENTAL PRINCIPLE A: Responsibility of the State)

4.1.1. The State’s physical protection regime is intended for all nuclear material in use and storage and during transport and for all nuclear facilities. The State should ensure the protection of nuclear material and nuclear facilities against unauthorized removal of nuclear material and against sabotage.

4.1.2. The State’s physical protection regime should be reviewed and updated regularly to reflect changes in the threat and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of nuclear material and nuclear facilities.

4.2. 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. (FUNDAMENTAL PRINCIPLE B: Responsibilities during International Transport)

4.2.1. A State’s responsibility for physical protection should be determined either by the borders of its sovereign territory or the flag of registration of the transport vessel or aircraft. A State’s physical protection regime for nuclear material in international transport should extend to the carriage of material on board ships or aircraft registered to that State while in international waters or airspace.

4.2.2. The State’s physical protection regime should ensure that nuclear material is always under the jurisdiction and continuous control of the State and that the point at which responsibility for physical protection is transferred from one State to another and from one carrier to another is clearly defined and implemented by all concerned. International transport operations should be overseen by one or more government organizations having the relevant authority and competence in transport security and/or the appropriate mode of transport.

4.2.3. The shipping State should consider, before allowing the international transport, if the States involved in the transport, including the transit States:

- are Parties to the Convention on the Physical Protection of Nuclear Material (INFCIRC/274 Rev.1); or
- have concluded with it a formal agreement which ensures that physical protection arrangements are implemented in accordance with internationally accepted guidelines; or
- formally declare that their physical protection arrangements are implemented according to internationally accepted guidelines; or
- have issued licences or other authorized documents which contain appropriate physical protection provisions for the transport of nuclear material.

4.2.4. When international shipments transit the territory of States, except when exercising the right of innocent passage through another State’s territorial sea, other than the shipping State and the receiving State, the shipping State should, in advance, identify and inform the other States involved in such transit in order that the transit States can ensure that the proposed arrangements are in accordance with their national law.

4.2.5. During international transport of Category I nuclear material, and possibly other categories of nuclear material, especially if accompanied by armed guards, the responsibility for physical protection measures should be the subject of formal agreement between the States concerned. The relevant competent authorities of the shipping, receiving, and transit States, and the flag State of the conveyance should establish specific measures to ensure the maintenance of communication regarding the continued integrity of the shipment in order to ensure that responsibility for response planning and capabilities is defined and fulfilled. Additionally, any sensitive information shared by States concerned should be protected and the overall arrangements for the shipment should be in accordance with the relevant States’ national laws. The point at which responsibility for physical
protection is transferred from one State to another should be stated in advance and in sufficient time to enable the receiving State to make adequate physical protection arrangements.

4.3. Assignment of physical protection responsibilities

4.3.1. The State should clearly define and assign physical protection responsibilities within all levels of government and for operators and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State’s physical protection regime. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the operator.

4.4. Legislative and regulatory framework

4.4.1. 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. (FUNDAMENTAL PRINCIPLE C: Legislative and Regulatory Framework)

4.4.1.1. A State should take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State’s physical protection regime.

4.4.1.2. The State should define requirements - based on threat assessment or design basis threat - for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal of nuclear material or sabotage. The State should ensure that the more stringent requirements for physical protection - either those against unauthorized removal of nuclear material or those against sabotage - are applied.

4.4.1.3. The State’s legislation should provide for the regulation of physical protection and include a licensing requirement. The State should promulgate and review its comprehensive regulations for the physical protection of nuclear material and nuclear facilities regularly. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership.

4.4.1.4. The State should license activities only when they comply with its physical protection regulations. The State should make provisions for a detailed examination, made by the State’s competent authority, of proposed physical protection measures in order to evaluate them for approval of these activities prior to licensing, and whenever a significant change takes place, to ensure continued compliance with physical protection regulations.

4.4.1.5. The State should ensure that evaluations also include exercises to test the integrated system, including the training and readiness of guards and/or response forces.

4.4.1.6. Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a graded approach. In implementing this policy, the State should ensure that measures are in place to determine the trustworthiness of persons with authorized access to sensitive information or, as applicable, to nuclear material or nuclear facilities.

4.4.1.7. Enforcement of physical protection regulations should be a part of a State’s physical protection regime.

4.4.1.8. Sanctions against the unauthorized removal of nuclear material and against sabotage should be part of the State’s legislative or regulatory system.

4.4.1.9. The recommended physical protection measures in this publication should be additional to, and not a substitute for other measures established for nuclear safety, nuclear material accountancy and control or radiation protection purposes.

Nuclear Security Recommendations on NM - After TM
4.4.2. 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 fulfill 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. (FUNDAMENTAL PRINCIPLE D: Competent Authority)

4.4.2.1. The State’s competent authority(ies) should have a clearly defined legal status and be independent from applicants/operators/carriers and have the legal authority to enable it to perform its responsibilities and functions effectively.

4.4.2.2. The State’s competent authority should have access to information from the State's system for nuclear material accountancy and control.

4.4.2.3. The State’s competent authority should be responsible for verifying continued compliance with the physical protection regulations and licence conditions through regular inspections and for ensuring that corrective action is taken, when needed.

4.4.2.4. To ensure that physical protection measures are maintained in a condition capable of meeting the State’s regulations and of effectively responding to the State’s requirements for physical protection, the State’s competent authority should ensure that evaluations based on performance testing are conducted by operators at nuclear facilities and by shippers or carriers for transport. Evaluations should be reviewed by the State’s competent authority, and should include administrative and technical measures, such as testing of detection, assessment and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the competent authority should ensure that corrective action is taken by the operator and by the shipper or carrier.

4.4.2.5. The State’s physical protection regime should include requirements for timely reporting of nuclear security events and information which enables the State’s competent authority to be informed of any changes at nuclear facilities or related to transport of nuclear material, which may affect implementation of physical protection measures.

4.4.3. Responsibilities 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). (FUNDAMENTAL PRINCIPLE E: Responsibility of the Licence Holders)

4.4.3.1. In this publication, licence holders are distinguished as either operators or shippers, corresponding to facility operators or transport shippers, respectively.

4.4.3.2. The operator and/or carrier should comply with all applicable regulations and requirements established by the State and competent authority.

4.4.3.3. The operator and/or carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site response forces.

4.4.3.4. The operator should maintain control of and be able to account for all nuclear material at all times. Information from the system for nuclear material accountancy and control that indicates possible unauthorized removal of nuclear material should be communicated as soon as possible to the facility manager responsible for physical protection. The operator should report any confirmed accounting discrepancy in a timely manner as stipulated by the competent authority.

4.4.3.5. The operator should prepare a security plan as part of its application to obtain a license. The security plan should be based on the design basis threat or the threat assessment and should include sections dealing with design, evaluation, implementation, and maintenance of the physical protection system, and contingency plans. The competent authority should review and approve the security plan, the implementation of which should then be part of the licence conditions. The operator should implement the approved security plan. The operator should review the security plan regularly to ensure it remains consistent with the facility conditions and the
approved physical protection systems. The operator should submit an amendment to the security plan for prior approval by the competent authority before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The competent authority should verify the operator's compliance with the security plan.

4.4.3.6. For a new nuclear facility, the design should take physical protection into account as early as possible and also address the interface issues with safety and nuclear material accountancy and control to avoid any conflicts and to be supportive of each other. The operator should verify that the design of the physical protection system satisfies all requirements and should validate the effectiveness of physical protection measures.

4.4.3.7. The operator should develop and implement means and procedures for evaluations, including performance testing (periodic verification that administrative and technical measures continue to function or are capable of performing their functions when called upon to do so), and maintenance (keeping measures in good operating condition, including both preventive and corrective procedures) of the physical protection system.

4.4.3.8. Whenever the physical protection system is determined to be incapable of providing the required level of protection, the operator and/or carrier should immediately implement compensatory measures to provide adequate protection. The operator and/or shipper should then - within an agreed period - plan and implement corrective actions to be reviewed and approved by the competent authority.

4.5. International cooperation and assistance

4.5.1. States are encouraged to cooperate and consult, and to exchange information on physical protection techniques and practices, either directly or through international organizations.

4.5.2. States should inform the International Atomic Energy Agency, and other States as applicable, of appropriate points of contact for matters related to the physical protection of nuclear material and nuclear facilities.

4.5.3. In the case of unauthorized removal or sabotage or credible threat thereof, the State should provide appropriate information as soon as possible to other States which appear to it to be concerned, and to inform, where appropriate, the International Atomic Energy Agency and other relevant international organizations.

4.5.4. States concerned should, in accordance with their national law, provide cooperation and assistance to the maximum feasible extent in the location and recovery of nuclear material to any State that so requests.

4.6. Identification and assessment of threats

The State’s physical protection should be based on the State’s current evaluation of the threat. (FUNDAMENTAL PRINCIPLE G: Threat)

4.6.1. The appropriate State authorities, using various credible information sources, should define the threat and associated capabilities in the form of a threat assessment and, if appropriate, a design basis threat. A design basis threat is developed from an evaluation by the State of the threat of unauthorized removal and of sabotage.

4.6.2. The State should ensure that the competent authority has access to information from other organizations in the State on present and foreseeable threats to nuclear activities.

4.6.3. When considering the threat, due attention should be paid to the insider. Insiders present a unique problem. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The physical protection system should be assisted by nuclear material accountancy and control measures to detect the protracted theft of nuclear material by an insider.

4.6.4. The State's physical protection regime should be based on a design basis threat for nuclear material and nuclear facilities with potential risk of high consequences, specifically for:

- unauthorized removal of Category I nuclear material (defined in Chapter 5),
- sabotage of nuclear material and nuclear facilities that have potentially high radiological consequences.

The State should decide whether to use a design basis threat or threat assessment for other nuclear material and nuclear facilities.
4.6.5. The State’s competent authority should use a threat assessment and/or a design basis threat as a common basis for the design and implementation of physical protection systems by the operator and/or carrier and its approval by the competent authority. The State should consider whether or not the threat assessment and/or design basis threat are the same for nuclear facilities and for transport.

4.6.6. The State should continuously review the threat and evaluate the implications of any changes in the threat assessment or design basis threat. In the event of any changes, the State’s competent authority should take steps to ensure that the change is sufficiently reflected in the regulations and by the operator’s and/or carrier’s physical protection measures.

4.6.7. Changes in physical protection measures may be necessary to address changes in the threat. Short term compensatory measures should be based on the current threat assessment, recognizing that a revision of the design basis threat may take additional time in this process. The effectiveness of these measures against the current threat should be evaluated. The design basis threat should then be reviewed in the light of the revised threat.

4.7. Risk-based physical protection measures and functions

4.7.1. Risk management

4.7.1.1. The State should ensure that the State’s physical protection regime is capable of establishing and maintaining the risk of unauthorized removal and sabotage at acceptable levels through risk management. This requires assessing the threat and the potential consequences of malicious acts, and then developing a legislative regulatory and programmatic framework that ensures appropriate effective physical protection measures are put in place.

4.7.1.2. Risk can be managed by:
   • reducing the threat. The threat may be reduced, for example, by the deterrence of robust physical protection measures, or the confidentiality of sensitive information;
   • improving the effectiveness of the physical protection systems. The physical protection system effectiveness may be increased, for example, by defence in depth or nuclear security culture; and
   • reducing the potential consequences of malicious acts by modifying specific contributing factors, for example, the amount and type of nuclear material and the design of the facility.

4.7.2. 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 nuclear material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities. (FUNDAMENTAL PRINCIPLE H: Graded Approach)

4.7.2.1. A graded approach is used to provide higher levels of protection against events that could result in higher consequences. The State should decide what level of risk is acceptable and what level of protection against the threat should be provided.

4.7.2.2. For protection against unauthorized removal of nuclear material, the State should regulate the categorization of nuclear material in order to ensure an appropriate relationship between the nuclear material of concern and the physical protection measures. For protection against sabotage, the State should establish its threshold(s) of unacceptable radiological consequences in order to determine an appropriate level of physical protection taking into account existing nuclear safety and radiological protection.

4.7.3. 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. (FUNDAMENTAL PRINCIPLE I: Defence in Depth)

4.7.3.1. State requirements for physical protection should be based on the concept of defence in depth. 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 facility design (including layout).

4.7.3.2. The three physical protection functions of detection, delay, and response should each use defence in depth and apply a graded approach to provide effective protection against the threat or design basis threat.

4.7.3.3. Defence in depth should take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats.

4.8. Sustaining the physical protection regime

4.8.1. 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. (FUNDAMENTAL PRINCIPLE F: Security Culture)

4.8.1.1. The foundation of nuclear security culture should be the recognition that a credible threat exists, that preserving nuclear security is important, and that the role of the individual is important.

4.8.1.2. The four component groups – the State, organizations, managers in organizations and individuals - should work together to develop and maintain an effective nuclear security culture.

4.8.1.3. The State should promote a nuclear security culture and encourage all security organizations to establish and maintain one. Nuclear security culture should be pervasive in all elements of the physical protection regime.

4.8.1.4. All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management’s commitment to provide guidelines to the staff and to set out the organization’s security objectives. Nuclear security culture should not be confined only to the organizations concerned and their personnel. All personnel should be regularly educated about physical protection as appropriate.

4.8.2. 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. (FUNDAMENTAL PRINCIPLE J: Quality Assurance).

4.8.2.1. The quality assurance policy and programmes for physical protection should ensure that a physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or design basis threat and that it meets the State’s regulations, including its prescriptive and/or performance-based requirements.

4.8.3. 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. (FUNDAMENTAL PRINCIPLE L: Confidentiality)

4.8.3.1. The State should take steps to ensure appropriate protection of specific or detailed information the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities. It should specify what information needs to be protected and how it should be protected, using a graded approach.

4.8.3.2. Management of physical protection systems should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in physical protection systems should be highly protected as it could indicate means of successfully removing nuclear material or of carrying out sabotage.

4.8.3.3. Sanctions against persons violating confidentiality should be part of the State’s legislative or regulatory system.
4.8.4. **Sustainability programme**

4.8.4.1. The State should establish a sustainability programme to ensure its physical protection regime is effective in the long term by committing the necessary resources.

4.8.4.2. Operators and carriers should establish sustainability programmes for their physical protection systems. Sustainability programmes should encompass:

- operating procedures (instructions);
- human resource management and training;
- equipment updating, maintenance, repair, and calibration;
- *performance testing* and operational monitoring;
- configuration management (The process of identifying and documenting the characteristics of a facility's physical protection system - including computer systems and software -, and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation);
- resource allocation and operational cost analysis.

4.9. Planning and preparedness for and response to nuclear security events

**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. (Fundamental Principle K: Contingency Plans).

4.9.1. The State’s competent authority should ensure that the operator prepares contingency plans of action to effectively counter the threat or design basis threat, including acts of actual or attempted unauthorized removal of nuclear material or sabotage, taking actions of the response forces into consideration.

4.9.2. The contingency plan should be approved by the State’s competent authority as a part of the security plan.

4.9.3. The coordination between the guards and response forces during a nuclear security event should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the guards, response forces and other response teams for implementation of the plans.

4.9.4. Arrangements should be made to ensure that during emergency conditions (including exercises), the effectiveness of the physical protection system is maintained.

4.9.5. The operator should initiate its contingency plan after detection and assessment of any malicious act.
5. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE

5.1. General

5.1.1. Basis for concern

An objective of the State’s physical protection regime is to prevent the unauthorized removal of nuclear material. An associated objective of the State’s physical protection regime, also addressed in this chapter, is to ensure the implementation of rapid and comprehensive measures to locate and recover missing or stolen nuclear material. Measures to locate and recover nuclear material after the reporting of it as lost, missing or stolen to a competent authority are addressed in Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control [4].

Levels of protection defined in this chapter are based on categorization of nuclear material for use in the construction of a nuclear explosive device. However, nuclear material is radioactive material, which has also to be protected against unauthorized removal that could have serious consequences if dispersed or used otherwise for malicious purpose. Protection requirements against unauthorized removal of nuclear material for potential subsequent offsite radiological dispersal are provided in the Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3]. These two sets of requirements for protection against unauthorized removal of nuclear material should be considered and implemented in a manner that the more stringent requirements for physical protection are applied.

When implementing requirements for protection against unauthorized removal, the requirements for the protection against sabotage addressed in Chapter 6 should also be taken into account. Appropriate physical protection measures should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

5.1.2. Categorization

5.1.2.1. The primary factor in determining the physical protection measures against unauthorized removal of nuclear material is the nuclear material itself. The table on the next page categorizes the different types of nuclear material e.g. plutonium, uranium; isotopic composition, according to content of fissile isotopes; physical and chemical form; degree of dilution; radiation level; and quantity. This categorization is the basis for a graded approach for protection against unauthorized removal of nuclear material that could be used in a nuclear explosive device.

5.1.2.2. According to footnote “e” of the categorization table, the protection of nuclear material with a radiation level that exceeds 1 Gy/hr (100 rad/hr) at one meter unshielded, which is classified as Category I or II before irradiation, may be reduced one category level below that determined by the fissile content of the material. However, if the threat assessment or design basis threat includes an adversary who is willing to die to accomplish their mission, States should carefully consider whether or not to reduce the categorization levels of the material on the basis of radiation levels sufficient to incapacitate the adversary before the malicious act is completed.

5.1.2.3. Nuclear material, which is in a form that is no longer usable for any nuclear activity, minimizes environmental dispersal and is practicably irrecoverable, may be protected against unauthorized removal in accordance with prudent management practices.

5.1.2.4. In determining the levels of physical protection in a facility, which may consist of several buildings, the operator may identify, in agreement with the State’s competent authority, part of the nuclear facility which contains nuclear material of a different category and which is therefore protected at a different level than the rest of the nuclear facility. Conversely, consideration may need to be given to adding together the total amount of nuclear material contained in a number of buildings to determine the appropriate protection arrangements for this group of buildings.
NOTE: This table is not to be used or interpreted independently of the text of the entire document.

<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></td>
<td>All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.</td>
<td></td>
<td></td>
<td></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></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- uranium enriched to 10% $^{235}$U but less than 20 % $^{235}$U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- uranium enriched above natural, but less than 10 % $^{235}$U</td>
<td></td>
<td></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>Unirradiated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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)</td>
<td>Depleted or natural uranium, thorium or low-enriched fuel(less than 10% fissile content)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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 meter 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 meter unshielded.
5.2. Requirements for physical protection against unauthorized removal of nuclear material in use and storage

5.2.1. General

5.2.1.2. The physical protection system of a nuclear facility should be integrated and effective against both sabotage and unauthorized removal of nuclear material.

5.2.1.3. Computer-based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the design basis threat or threat assessment.

5.2.1.4. The operator should assess and manage the physical protection interface with safety and nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

5.2.1.5. Nuclear material, which is required to be protected in accordance with prudent management practice should be secured against unauthorized removal and unauthorized access.

5.2.2. Requirements for Categories I, II and III nuclear material

In addition to the requirements above, the following requirements apply to Categories I, II and III nuclear material.

5.2.2.1. Nuclear material should be used or stored within at least a limited access area.

5.2.2.2. Provision should be made for detecting unauthorized intrusion and for appropriate action by guards or response forces to attempted intrusions.

5.2.2.3. Every nuclear material handler should be required to conform to procedures for transferring custody of the nuclear material to the succeeding handler. Additionally, nuclear material handlers should endeavour to ascertain on reporting for duty that no interference with or unauthorized removal of nuclear material has taken place.

5.2.2.4. Technical means and procedures for access control, such as keys and computerized access lists, should be protected against compromise, e.g. manipulation or falsification.

5.2.2.5. Movements of Category III nuclear material within a limited access area should be the responsibility of the operator, who should apply all prudent and necessary physical protection measures.

5.2.2.6. Contingency plans should be prepared to counter malicious acts effectively and to provide for appropriate response by guards or response forces. Such plans should also provide for the training of facility personnel in their actions.

5.2.3. Requirements for Categories I and II nuclear material

In addition to the requirements above, the following requirements apply to Categories I and II nuclear material.

5.2.3.1. Nuclear material should be used or stored within at least a protected area.

5.2.3.2. A protected area should be located inside a limited access area. The protected area perimeter should be equipped with a physical barrier, intrusion detection and assessment to detect unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken.

5.2.3.3. The number of access points into the protected area should be kept to the minimum necessary. All points of potential access should be appropriately secured and alarmed.

5.2.3.4. Vehicles, persons and packages entering and leaving the protected area should be subject to search for detection and prevention of unauthorized access and of introduction of prohibited items or removal of nuclear material, as appropriate. Entry of vehicles into the protected area should be strictly minimized and limited to designated parking areas.
5.2.3.5. Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Persons authorized for unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors should be escorted by persons authorized for unescorted access.

5.2.3.6. The identity of authorized persons entering the *protected area* should be verified. Passes or badges should be issued and visibly displayed inside the *protected area*.

5.2.3.7. A record should be kept of all persons having access to or possession of keys, key-cards and/or other systems, including computer systems that control access to *nuclear material*.

5.2.3.8. On-site movements between two *protected areas* should be treated in compliance with the requirements for *nuclear material* during *transport*, after taking into account existing facilities *physical protection measures*.

5.2.3.9. A permanently staffed *central alarm station* should be provided, for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled.

5.2.3.10. Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification.

5.2.3.11. Dedicated, redundant, secure and diverse transmission systems for two-way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two-way secure voice communication should be provided between *guards* and the *central alarm station*.

5.2.3.12. A 24-hour *guarding service and response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing a *malicious act*. The *central alarm station* personnel should report at scheduled intervals to the off-site *response forces*. The *guards* and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations.

5.2.3.13. The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

- deter an adversary,
- detect intrusion,
- inspect visually the physical protection components,
- supplement the existing *physical protection measures*, and
- provide an initial response.

5.2.3.14. Evaluations - including *performance testing* of the implemented *physical protection measures* and integrated *physical protection system* and of timely response of the *guards* and *response forces* - should be conducted regularly to determine the reliability and the effectiveness against the *threat* and to detect any equipment malfunction. These should be carried out with full cooperation between the *operator* and *response forces*. Significant deficiencies and action taken should be reported as stipulated by the *competent authority*.

5.2.4. **Requirements for Category I nuclear material**

In addition to the requirements above, the following requirements apply to Category I *nuclear material*.

5.2.4.1. *Nuclear material* should be used or stored within an *inner area*. An *inner area* could also be a *vital area*.

5.2.4.2. An *inner area* should provide an additional layer to the *protected area* for *detection*, access control and delay against *unauthorized removal*. *Inner areas* should be appropriately secured and alarmed when unattended.
5.2.4.3. **Inner areas** should provide delay against unauthorized access to allow for a timely and appropriate response to a malicious act. Delay measures should be designed considering both insiders’ and external adversaries’ capabilities, and should take into account and be balanced for all potential points of intrusion.

5.2.4.4. Vehicle barriers should be installed at an appropriate distance from the inner area to prevent the penetration of unauthorized land and waterborne vehicles specified in the design basis threat that could be used by an adversary for committing a malicious act. Attention should also be given to providing protection measures against any airborne threat specified in the design basis threat for the operator.

5.2.4.5. Only authorized persons should have access to the inner area. Effective access control measures should be taken to ensure the detection and prevention of unauthorized access. The number of authorized persons entering the inner area should be kept to the minimum necessary. Persons with authorized access to the inner area should be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized unescorted access.

5.2.4.6. Vehicles, persons and packages should be subject to search on entering both the protected and inner areas for detection and prevention of unauthorized access and of introduction of prohibited items. Vehicles, persons and packages leaving the inner area should be subject to search for detection and prevention of removal of nuclear material. Instruments for the detection of nuclear material, metals, and explosives can be used for such searches.

5.2.4.7. Private vehicles should be prohibited access to inner areas.

5.2.4.8. The number of access points to the inner areas should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and alarmed.

5.2.4.9. A record should be kept of all persons having access to or possession of keys, key-cards and/or other systems, including computer systems, that control access to nuclear material or to inner areas.

5.2.4.10. Inside the inner area, nuclear material should be stored in a hardened room (‘strong room’) or hardened enclosure that provides an additional layer of detection and delay against removing the material. This storage area should be locked and alarms activated except during authorized access to the material. When nuclear material is kept in an unoccupied work area outside this storage area, e.g. overnight, equivalent compensatory physical protection measures should be established.

5.2.4.11. Provisions, including redundancy measures, should be in place to ensure that the central alarm stations’ functions in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station).

5.2.4.12. To counter the insider threat, whenever an inner area is occupied, detection of unauthorized action should be achieved by constant surveillance (e.g. the two-person rule).

5.2.4.13. At least annually, performance testing of the full scope physical protection system for Category I nuclear material should include appropriate exercises, for example force-on-force exercises to determine if the response forces can provide an effective and timely response to prevent the unauthorized removal of nuclear material.

5.3. Requirements for measures to locate and recover missing or stolen nuclear material

5.3.1. Scope and boundary

This section provides requirements for the State and operator that should participate in a coordinated response for the location and recovery of missing or stolen nuclear material. For the operator, these location and recovery measures should include on-site operations and appropriate assistance to the State organizations for off-site operations.

5.3.2. Requirements for the State

5.3.2.1. The State should ensure that its physical protection regime includes rapid response and comprehensive measures to locate and recover missing or stolen nuclear material. These location and recovery measures should include on-site and off-site operations.
5.3.2.2. The State should define the roles and responsibilities of appropriate State response organizations, operators and/or carriers to locate and to recover any missing or stolen nuclear material. 

5.3.2.3. The State should ensure that contingency plans - including interfaces with safety, as appropriate - are established by operators and/or carriers to locate and to recover any missing or stolen nuclear material. 

5.3.2.4. The responsible State organizations should develop comprehensive plans for the rapid location and recovery of nuclear material which has been declared missing or stolen from facilities or transport. 

5.3.2.5. For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations and operators and/or carriers. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations. 

5.3.2.6. The State should ensure that operators and/or carriers and State organizations conduct exercises to assess and validate the plans prepared by the operators and/or carriers and the State organizations, and also to train the various participants how to react in such a situation. 

5.3.2.7. The State should ensure that plans for location and recovery are regularly reviewed and updated. 

5.3.3. Requirements for the operator 

The requirements for the operator are organized by the following process for the location and recovery of missing or stolen nuclear material. The steps in this process include detection, confirmation, declaration, location, securing and return of the missing or stolen nuclear material. 

5.3.3.1. Detection of missing or stolen nuclear material 

The operator should ensure that any missing or stolen nuclear material is detected in a timely manner by means such as the system for nuclear material accountancy and control and the physical protection system (e.g. periodic inventories, inspections, access control searches, radiation detection screening). 

The operator’s manager responsible for physical protection should be informed as soon as the nuclear material is suspected or discovered to be missing or stolen. 

5.3.3.2. Confirmation of missing or stolen nuclear material 

The operator should confirm any missing or stolen nuclear material by means of a rapid emergency inventory as soon as possible within the time period specified by the State. A system for nuclear material accountancy and control should provide accurate information about the missing nuclear material in the facility following a nuclear security event. 

5.3.3.3. Declaration of missing or stolen nuclear material 

The operator should notify the competent authority and other relevant State organizations of missing or stolen nuclear material as specified by the State. 

5.3.3.4. Contingency plan 

The operator’s measures to locate and recover missing or stolen nuclear material should be included in its contingency plan, and should be regularly tested and evaluated. Appropriate joint exercises should be held with the competent authority and other State organizations. 

5.3.3.5. Actions to locate missing or stolen nuclear material 

The operator should take all appropriate measures to locate, as soon as possible, any declared missing or stolen nuclear material on site and possibly off site (in hot pursuit) when authorized as approved in the contingency plan. 

5.3.3.6. Actions to secure and return missing or stolen nuclear material 

As soon as possible after the missing or stolen nuclear material has been located and identified, the operator should, in accordance with the contingency plan, secure this material in situ and then return it to a nuclear facility with due authorization from the competent authority. 

Nuclear Security Recommendations on NM - After TM
5.3.3.7. Operator assistance

The operator should provide any other necessary assistance to the State organizations to locate and recover nuclear material and should cooperate during subsequent investigations and prosecution.
6. REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR FACILITIES AND NUCLEAR MATERIAL IN USE AND STORAGE

6.1. General

An objective of the State's physical protection regime is to prevent sabotage on site. An associated objective of the State's physical protection regime also addressed in this chapter is to ensure the implementation of rapid and comprehensive measures to mitigate or minimize the radiological consequences of sabotage, taking emergency plans into account. This chapter applies to nuclear facilities, including nuclear reactors (nuclear power plants and research reactors) and nuclear fuel cycle facilities (including conversion, enrichment, fabrication, reprocessing, and storage facilities). Nuclear facilities frequently contain other hazardous material that could have severe non-radiological consequences. This chapter does not address such material.

The recommendations for physical protection measures in this chapter are made on the basis of the potential radiological consequences resulting from an act of sabotage. The categorization specified in Chapter 5 is based on the attractiveness of material for the potential construction of a nuclear explosive device, and cannot be directly applied to protection against sabotage.

When implementing requirements for protection against sabotage, the requirements for the protection against unauthorized removal addressed in Chapter 5 should also be taken into account. Appropriate physical protection measures should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

6.2. Basis for graded approach for physical protection against sabotage

This section presents the approach to be used to define the nuclear facilities and nuclear material which require protection against sabotage.

6.2.1. For each nuclear facility, an analysis, validated by the competent authority, should be performed to determine whether the radioactive inventory has the potential to result in unacceptable radiological consequences as determined by the State, assuming that the sabotage acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures.

6.2.2. On the basis of these analyses, the State should consider the range of radiological consequences that can be associated with all its nuclear facilities and should appropriately grade the radiological consequences that exceed its limits for unacceptable radiological consequences for assigning appropriate levels of protection.

6.2.3. In accordance with the fundamental principle of the graded approach to physical protection, the State should define a set of physical protection design objectives and/or measures for each assigned level of protection.

6.2.4. If the potential radiological consequences of sabotage are less severe than the State's unacceptable radiological consequences, then the operator should protect safety related equipment and devices by controlling access to them and securing them.

6.2.5. If the potential radiological consequences of sabotage exceed the State’s unacceptable radiological consequences, then the operator should identify equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences.

6.3. Requirements for process to design physical protection systems against sabotage

This section presents the process to be used to design the physical protection system of a nuclear facility and nuclear material which require protection against sabotage.

6.3.1. Using the threat assessment or design basis threat, the operator - in cooperation with the State’s competent authority - should define credible scenarios by which adversaries could sabotage nuclear facilities and nuclear material.

6.3.2. When defining scenarios, the operator should consider the location of the nuclear facility and all nuclear material and other radioactive materials including radioactive waste, especially those at the same location inside a nuclear facility.
6.3.3. Sabotage scenarios should consider external and/or insider adversaries who attempt to damage or to manipulate nuclear material and other radioactive material or equipment, systems, structures, components or devices, including possible stand-off attack, consistent with the State’s threat assessment or design basis threat.

6.3.4. The operator should design a physical protection system that is effective against the defined sabotage scenarios and complies with the required level of protection for the nuclear facility and nuclear material.

6.3.5. The physical protection system against sabotage should be designed as an element of an integrated system to prevent the potential consequences of sabotage by taking into account the robustness of the engineered safety and operational features, and the fire protection, radiation protection and emergency preparedness measures.

6.3.6. The physical protection system should be designed to deny unauthorized access of persons or equipment to the targets, minimize opportunity of insiders, and to protect the targets against possible stand-off attacks consistent with the State’s threat assessment or design basis threat. The response strategy should include denial of adversary access to the sabotage targets or denial of adversary task completion at the sabotage targets. Denying access to the targets is accomplished by the primary physical protection functions of detection, delay and response; whereas protecting against stand-off attacks involves facility design considerations, barrier design considerations to implement stand-off distance, and other disruption measures.

6.3.7. The operator should evaluate and the State should validate the design of physical protection system effectiveness to verify that it complies with the required level of protection for the nuclear facility and nuclear material. This evaluation should include performance testing of the physical protection system and of the timely response of the guards and response forces.

6.3.8. If the evaluation of the design of physical protection system indicates that it is ineffective, then the operator should redesign the physical protection system and re-evaluate its effectiveness.

6.3.9. The physical protection system of a nuclear facility should be integrated and effective against both sabotage and unauthorized removal of nuclear material.

6.3.10. The operator should assess and manage the physical protection interface with safety activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive. The results of safety analysis provide useful input, including target identification and potential radiological consequences, and should be considered during design of the physical protection system.

6.3.11. Computer-based systems used for physical protection, safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the design basis threat or threat assessment.

6.4. Requirements for physical protection against sabotage at nuclear facilities

This section provides requirements for nuclear facilities, including nuclear power plants, the sabotage of which could lead to high radiological consequences and for other nuclear facilities.

6.4.1. Requirements for high consequences facilities including nuclear power reactors

6.4.1.1. Because of their large inventory of highly radioactive fission products and their internal energy, nuclear power plants have potentially high radiological consequences and consequently need a high level of protection against sabotage.

6.4.1.2. The nuclear material and the equipment, systems or devices which if sabotaged could lead to high radiological consequences, should be located within one or more vital areas, located inside a protected area.

6.4.1.3. A protected area should be located inside a limited access area. The protected area perimeter should be equipped with a physical barrier, intrusion detection and assessment to detect unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken.

6.4.1.4. The number of access points into the protected area should be kept to the minimum necessary. All points of potential access should be appropriately secured and alarmed.
6.4.1.5. Vehicles, persons and packages entering and leaving the protected area should be subject to search for detection and prevention of unauthorized access and of introduction of prohibited items, as appropriate. Instruments for the detection of nuclear material, metal, and explosives can be used for such searches. Entry of vehicles into the protected area should be strictly minimized and limited to designated parking areas.

6.4.1.6. Only authorized persons should have access to the protected area. Effective access control measures should be taken to ensure the detection and prevention of unauthorized access. The number of authorized persons entering the protected area should be kept to the minimum necessary. Persons authorized for unescorted access to the protected area should be limited to those whose trustworthiness has been determined. Persons whose trustworthiness has not been determined, such as temporary repair, service or construction workers and visitors, should be escorted by persons authorized for unescorted access.

6.4.1.7. The identity of authorized persons entering the protected area should be verified. Passes or badges should be issued and visibly displayed inside the protected area.

6.4.1.8. A vital area should provide an additional layer to the protected area for detection, access control and delay against sabotage. Vital areas should be appropriately secured and alarmed when unattended.

6.4.1.9. Vital areas should provide delay against unauthorized access to allow for a timely and appropriate response to a malicious act. Delay measures should be designed considering both the insiders’ and external adversaries’ capabilities, and should take into account and be balanced for all potential points of intrusion.

6.4.1.10. The number of access points to the vital areas should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and alarmed.

6.4.1.11. To counter the insider threat, whenever persons are present in vital areas, provision should be made for timely detection of unauthorized action.

6.4.1.12. Vehicle barriers should be installed at an appropriate distance from the vital area to prevent the penetration of unauthorized land and waterborne vehicles specified in the design basis threat that could be used by an adversary for committing a malicious act. Consideration should also be given to providing protection measures against any airborne threat specified in the design basis threat for the operator.

6.4.1.13. Only authorized persons should have access to the vital area. Effective access control measures should be taken to ensure the detection and prevention of unauthorized access. The number of authorized persons entering the vital area should be kept to the minimum necessary. Persons authorized for access to the vital area should be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access.

6.4.1.14. Private vehicles should be prohibited access to vital areas.

6.4.1.15. Timely detection of tampering or interference with vital area equipment, systems or devices should be provided. A timely report should be made to the competent authority whenever there is reason to suspect that any malicious activity has occurred.

6.4.1.16. During a shutdown/maintenance period, strict access control to vital areas should be maintained. Prior to reactor startup, searches and testing should be conducted to detect any tampering that may have been committed during shutdown/maintenance.

6.4.1.17. A record should be kept of all persons having access to or possession of keys, key-cards and/or other systems, including computer systems, that control access to nuclear material or to vital areas.

6.4.1.18. A permanently staffed central alarm station should be provided where a protected area is needed, for monitoring and assessment of alarms, initiation of response, and communication with the guards, response forces, and facility management. Information acquired at the central alarm station should be stored in a secure manner. The central alarm station should normally be located in a protected area and protected so that its functions can continue in the presence of a threat, e.g. hardened. Access to the central alarm station should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the central alarm stations’ key functions can continue during an emergency (e.g. backup alarm station).
6.4.1.19. Alarm equipment, alarm communication paths, and the central alarm station should be provided with an uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification.

6.4.1.20. Dedicated, redundant, secure and diverse transmission systems for two-way voice communication between the central alarm station and the response forces should be provided for activities involving detection, assessment and response. Dedicated two-way secure voice communication should be provided between guards and the central alarm station.

6.4.1.21. A 24-hour guarding service and response forces should be provided to ensure an adequate and timely response to prevent an adversary from completing a malicious act. The central alarm station personnel should report at scheduled intervals to the off-site response forces. The guards and response forces should be trained and adequately equipped for their function in accordance with national laws and regulations.

6.4.1.22. The guards should conduct random patrols of the protected area. The main functions of the patrols should be to:

- deter an adversary,
- detect intrusion,
- inspect visually the physical protection components,
- supplement the existing physical protection measures; and
- provide initial response.

6.4.1.23. Evaluations - including performance testing, of the individual physical protection measures and integrated physical protection system and of timely response of the guards and response forces - should be conducted regularly to determine the reliability and the effectiveness against the threat and to detect any equipment malfunction. These should be carried out with full cooperation between the operator and response forces. Performance testing of the integrated physical protection system should include appropriate exercises, for example force-on-force exercises, to determine if the response forces can provide an effective and timely response to prevent sabotage. Significant deficiencies and action taken should be reported as stipulated by the competent authority.

6.4.1.24. Contingency plans should be prepared to effectively counter malicious acts and to provide for appropriate response by guards or response forces. Such plans should also provide for the training of facility personnel in their actions.

6.4.2. Requirements for other nuclear facilities and nuclear material

6.4.2.1. Sabotage of nuclear facilities other than high consequences facilities and of various forms and quantities of nuclear material could also result in radiological hazards to the public. States should determine the level of protection needed against such sabotage depending upon the degree of radiological consequences. Measures specified in Section 6.4.1. may be applied as appropriate.

6.5. Requirements for associated measures to mitigate or minimize consequences of sabotage

6.5.1. Scope and boundary

This section provides requirements for the State and operator, who should participate in a coordinated manner to respond to an act of sabotage to mitigate or minimize radiological consequences. In case of attempted sabotage or sabotage which could affect a nuclear facility, two kinds of measures should be taken by the appropriate State response organizations and the operator. The contingency plan should include measures which focus on preventing further damage, on securing the nuclear facility and on protecting emergency equipment and personnel. The emergency plan consists of measures to ensure the mitigation or minimization of the radiological consequences of sabotage as well as human errors, equipment failures and natural disasters. These plans should be comprehensive and complementary.
6.5.2. Requirements for the State

6.5.2.1. The State should define the roles and responsibilities of appropriate State response organizations, operators and/or carriers to prevent further damage, secure the nuclear facility and transport and protect emergency equipment and personnel.

6.5.2.2. The State should establish a contingency plan to prevent further damage, secure the nuclear facility and transport and protect emergency equipment and personnel. This plan should support and supplement the contingency plan prepared by operator.

6.5.2.3. The State should ensure that contingency plans are established by operators and carriers, which are approved by the competent authority.

6.5.2.4. The contingency plans of the State and of the operators/carriers should include a description of the objectives, policy and concept of operations for the response to attempted sabotage or sabotage, and of the structure, authorities and responsibilities for a systematic, coordinated and effective response.

6.5.2.5. The State should develop arrangements and protocols among appropriate State response organizations and operators and/or carriers, for the coordination of measures for preventing further damage, securing the nuclear facility and transport and protecting emergency equipment and personnel. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations.

6.5.2.6. The State should ensure that operators and/or carriers and appropriate State response organizations conduct exercises to assess and validate the contingency plans prepared by the operators and/or carriers and the State organizations, and also to train the various participants how to react in such a situation.

6.5.2.7. The State should ensure that contingency plans are regularly reviewed and updated.

6.5.2.8. Joint exercises that simultaneously test emergency and contingency plans and actions should be regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems.

6.5.2.9. The State should ensure that response forces are familiarized with the site and sabotage targets and have adequate knowledge on radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety.

6.5.3. Requirements for operator

6.5.3.1. The operator should establish a contingency plan to prevent further damage, secure the nuclear facility and protect emergency equipment and personnel.

6.5.3.2. The operator should prepare facility personnel to act in full coordination with guards, response forces, law enforcement agencies and safety response teams for implementing the contingency plans.

6.5.3.3. The operator should assess, on detection of a malicious act, whether this act could lead to radiological consequences.

6.5.3.4. The operator should notify, in a timely manner, the competent authority, response forces and other relevant State organizations, of attempted sabotage or sabotage as specified in the contingency plan.
7. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT

7.1. Requirements for physical protection of nuclear material against unauthorized removal during transport

Levels of protection defined in this section are based on categorization of nuclear material for use in the construction of a nuclear explosive device. However, nuclear material is radioactive material, which has also to be protected against unauthorized removal that could have serious consequences if dispersed or used otherwise for malicious purpose. Protection requirements against unauthorized removal of nuclear material for potential subsequent offsite radiological dispersal are provided in the Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3]. These two sets of requirements for protection against unauthorized removal of nuclear material should be considered and implemented in a manner that the more stringent requirements for physical protection are applied.

Before implementing requirements for protection against unauthorized removal, the requirements for the protection against sabotage addressed in Section 7.3 should also be taken into account. Appropriate physical protection measures should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner.

7.1.1. General

7.1.1.1. Nuclear material may be more vulnerable to unauthorized removal during transport than while it is located within a nuclear facility.

7.1.1.2. The categorization table in Chapter 5 is the basis for a graded approach for protection against unauthorized removal during transport of nuclear material that could be used in a nuclear explosive device.

7.1.1.3. The total amount of nuclear material on or in a single conveyance should be used to determine an aggregate categorization and identify the appropriate protection arrangements for the conveyance. When different types of nuclear material are transported on the same conveyance, an appropriate aggregation formula should be used to determine the category of the consignment.

7.1.2. Common requirements for transport of nuclear material

7.1.2.1. Physical protection against unauthorized removal during transport should encompass, as far as operationally practicable in accordance with graded approach:

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

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

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;

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

i. Ensuring that packages and/or conveyance are not left unattended for any longer than is absolutely necessary.
7.1.2.2. 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. This requires great restraint 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. 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.

7.1.2.3. Before commencing an international shipment, the shipper should ensure that the arrangements are in accordance with the physical protection regulations of the receiving State and of other States which are transited.

7.1.2.4. Procedures should be established to ensure the security of keys to conveyances and security locks commensurate with the categorization of the transport being undertaken.

7.1.2.5. 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 in Section 5.2 for use and storage.

7.1.3. Requirements for Category I, II and III nuclear material

In addition to the requirements above, the following requirements apply to Categories I, II and III nuclear material.

7.1.3.1. The 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.

7.1.3.2. Physical protection during transport should include prior agreements among shipper, receiver, and carrier, specifying time, place and procedures for transferring physical protection responsibilities.

7.1.3.3. 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.

7.1.3.4. Where practicable, locks and seals should be applied to conveyances, compartments or freight containers. If locks and/or seals are used, checks should be made before dispatch and after any intermodal transfer of each nuclear material consignment, the integrity of the package and the locks and seals of the conveyance, compartment or freight container.

7.1.3.5. 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.

7.1.3.6. Physical protection measures should include communication from the conveyance capable of summoning appropriate responders.

7.1.3.7. 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.

7.1.4. Requirements for Category I and II nuclear material

In addition to the requirements above, the following requirements apply to Categories I and II nuclear material.

7.1.4.1. Physical protection measures should include surveillance of the cargo, load compartment or conveyance. States are encouraged to use guards for such surveillance.

7.1.4.2. The receiver should confirm readiness to accept delivery (and hand-over, if applicable) at the expected time, prior to the commencement of the shipment.
7.1.4.3. A transport security plan should be submitted by the shipper and/or carrier as appropriate to the competent authority for approval. This plan should include the route, with alternative routing as appropriate, stopping places, destination hand-over arrangements, identification of persons authorized to take delivery, accident procedures, and reporting procedures, both routine and emergency. In choosing the route, the capabilities of the response forces should be taken into account.

7.1.4.4. Prior to commencing transport, the carrier should verify that all physical protection measures are in place in accordance with the transport security plan.

7.1.4.5. 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. In these circumstances, when guards are not armed, compensating measures should be applied.

7.1.4.6. Physical protection measures should provide sufficient delay in the conveyance, freight container and/or package so that guards and/or response forces have time to intervene to prevent removal of the material.

7.1.4.7. The conveyance should be searched immediately prior to loading and shipment. 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.

7.1.4.8. When appropriate, personnel with physical protection responsibilities should be given written instructions, which have been approved by the competent authority, detailing their responsibilities during the transport.

7.1.4.9. Particular consideration should be given to ensuring confidentiality of information relating to transport operations, including dissemination only to persons with a need to know this information.

7.1.4.10. 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.

7.1.4.11. 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 of nuclear material.

7.1.4.12. Dependant on the mode of transport, the consignment should be shipped, by:
- road, under exclusive use conditions; or
- rail, where operationally practicable, in a freight train in an exclusive use fully enclosed, and locked conveyance; or
- water, in a secure compartment or container which is locked and sealed; or
- air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

While nuclear material is on board attending departure, provisions should be made for sufficient access delay or compensating measures to meet the threat assessment or design basis threat.

7.1.5. Requirements for Category I nuclear material

In addition to the requirements above, the following requirements apply to Category I nuclear material.

7.1.5.1. The approval by the competent authority of the transport security plan should be based on a detailed examination of proposed physical protection measures. The transport security plan should include arrangements for making changes, such as alteraion of the route during the shipment, in response to unexpected changes in the physical environment, threat and operating conditions.

7.1.5.2. A further authorization by the competent authority of the shipment should be required just prior to commencing transport and should be conditional on a 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.
7.1.5.3. Guards, appropriately equipped and trained, should accompany each shipment to protect the nuclear material against unauthorized removal, including surveillance of the route - before and during loading and unloading operations - for any threat indicators and 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. 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 and/or interior cargo area.

7.1.5.4. When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, significant compensating 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.

7.1.5.5. 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. While the shipment is in progress, the transport control centre should be staffed by qualified shipper or State designees whose trustworthiness has been predetermined.

7.1.5.6. 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.

7.1.5.7. The guard or conveyance crew should be instructed to report frequently and upon arrival at the destination and each overnight stopping place and place of hand-over of the shipment by secure two-way voice communications to the transport control centre.

7.1.5.8. For shipment by road, designated conveyance(s) should be used exclusively for each consignment and should preferably be specially designed to resist attack and equipped with a conveyance disabling device. Each conveyance should carry a guard or crew member in addition to the driver.

7.1.5.9. For shipment by road, each conveyance should be accompanied by at least one vehicle with guards to conduct a surveillance of the route for any threat indicators and to protect the conveyance and initiate an appropriate response.

7.1.5.10. During shipment by rail, accompanying guards should travel in close to the conveyance to have proper effective surveillance.

7.1.5.11. Shipment by water should be carried out by a dedicated transport vessel.

7.1.5.12. Shipment by air should be by aircraft designated for cargo only and for which the nuclear material is its sole cargo.

7.2. Requirements for measures to locate and recover nuclear material missing or stolen during transport

7.2.1. Scope and boundary

An objective of the State’s physical protection regime, addressed in this Chapter, is to ensure the implementation of rapid and comprehensive measures to locate and recover missing or stolen nuclear material. Measures to locate and recover nuclear material after the reporting of it as missing, lost or stolen to a competent authority are addressed in Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control [4].

7.2.2. Requirements for States

The requirements for the State are provided in Section 5.3.2.

7.2.3. Requirements for carrier

The requirements for the carrier are organized by the process for the discovery, location, and reporting of lost or stolen nuclear material.
7.2.3.1. Discovery of missing nuclear material
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.

7.2.3.2. Actions to locate packages
The carrier should take immediate action to determine if missing packages are misplaced but still under its control.

7.2.3.3. Reporting of missing nuclear material
If packages are determined to be missing or have been tampered with, the carrier should immediately report this to the shipper and relevant authorities.

7.2.3.4. Carrier assistance
The carrier should provide any requested assistance to the appropriate State organizations to locate and recover nuclear material and should cooperate during subsequent investigations and prosecution.

7.3. Requirements for physical protection of nuclear material against sabotage during transport
The recommendations for physical protection measures in this section are made on the basis of the potential radiological consequences resulting from an act of sabotage. The categorization specified in Chapter 5 is based on the attractiveness of material for the potential construction of a nuclear explosive device, and cannot be directly applied to protection against sabotage.
The transport of nuclear material may be more vulnerable to sabotage than nuclear facilities.
This section presents recommendations that should be used by the State, shippers, carriers, receivers, guards and response forces to help ensure protection of nuclear material during transport against sabotage.

7.3.1. When implementing requirements for protection against sabotage, the requirements for the protection against unauthorized removal addressed in Section 7.1 should also be taken into account. Appropriate physical protection measures should then be designed and implemented for both in an integrated manner.

7.3.2. In accordance with the fundamental principles of the graded approach to physical protection, the State should define protection requirements that correspond to the level of radiological consequences. The safety features of the design for the transport package, container and conveyance should be taken into account when deciding what additional physical protection measures are needed to protect the material against sabotage.

7.3.3. In determining the additional physical protection measures - based on threat assessment or design basis threat - to be applied to prevent sabotage of nuclear material during transport, consideration should be given to:

- postponing the shipment,
- rerouting the shipment to avoid high threat areas,
- enhancing the robustness of the package or the conveyance,
- detailed route surveillance to observe the current environment,
- providing (additional) guards.

7.4. Requirements for associated measures to mitigate and minimize the radiological consequences of sabotage during transport
7.4.1. Scope and boundary
An objective of the State’s physical protection regime addressed in this Section is to ensure the implementation of rapid and comprehensive measures to mitigate or minimize the radiological consequences of sabotage, taking into account emergency plans.
7.4.2. Requirements for States
The requirements for the State are provided in Section 6.5.2.

7.4.3. Requirements for carrier
7.4.3.1. The carrier’s contingency plan should include measures to mitigate and minimize the potential consequences of an act of sabotage.

7.4.3.2. The carrier should prepare transport personnel to act in full coordination with guards, law enforcement agencies and response teams for implementing the contingency plan.

7.4.3.3. The carrier’s transport control centre or management should be informed as soon as an attempt or an act of sabotage is detected.

7.4.3.4. The carrier should notify, in a timely manner, the shipper, the competent authority, response forces and other relevant State organizations, of attempted sabotage or sabotage as specified in the contingency plan.

7.4.3.5. Immediately following an act of sabotage, the carrier and/or guards should take measures to secure the transport and minimize the consequences of the act.

REFERENCES


