



Republic of the Philippines  
Department of Science and Technology  
**PHILIPPINE NUCLEAR RESEARCH INSTITUTE**  
Commonwealth Avenue, Diliman, Quezon City

## **CPR PART 32**

# **SECURITY REQUIREMENTS IN THE TRANSPORT OF NUCLEAR MATERIAL**

## **TABLE OF CONTENTS**

<b>I. GENERAL PROVISIONS.....</b>	<b>1</b>
Section 1. Purpose.....	1
Section 2. Scope.....	1
Section 3. Specific Exemptions.....	2
Section 4. Definitions.....	2
Section 5. Interpretation.....	5
Section 6. General Obligations.....	5
Section 7. Access to Premises and Information.....	5
Section 8. Resolution of Conflicts.....	5
Section 9. Additional Requirements.....	6
Section 10. Transport Requirements Addressed by Other National Modal Agencies.....	6
Section 11. Communication.....	6
<b>II. ADMINISTRATIVE REQUIREMENTS .....</b>	<b>6</b>
Section 12. Responsibilities of the Licensee.....	6
Section 13. Security Manager.....	7
Section 14. Security Culture.....	7
Section 15. Personnel Access Authorization.....	7
Section 16. Confidentiality and Information Security.....	8
Section 17. Trustworthiness of Individuals Involved in Transport Operation.....	8
Section 18. Training Requirements.....	9
Section 19. Transport Control Center (TCC).....	9
Section 20. Performance Testing and Verification of Compliance.....	9
<b>III. TECHNICAL REQUIREMENTS.....</b>	<b>10</b>
Section 21. Graded Approach.....	10
Section 22. Contingency Plan.....	10
Section 23. Physical Protection Program.....	10
Section 24. Review and Evaluation.....	11
Section 25. Transport Security Plan.....	11
<b>IV. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT.....</b>	<b>12</b>
Section 26. General Requirements.....	12
Section 27. Requirements for Category I, II and III Nuclear Material.....	12
Section 28. Requirements for Category I and II Nuclear Material.....	14
Section 29. Requirements for Category I Nuclear Material.....	15
Section 30. Nuclear Material that Poses Radiological Risk.....	18

Section 31. Measures to Locate and Recover Missing or Stolen Nuclear Material during Transport.....	18
Section 32. Measures for Protection against Sabotage.....	19
Section 33. Measures to Mitigate or Minimize the Radiological Consequences of Sabotage.....	19
<b>V. RECORDING AND REPORTING REQUIREMENTS .....</b>	<b>19</b>
Section 34. Inventories and Records.....	19
Section 35. Reporting Requirements.....	20
Section 36. Notification of Incidents.....	20
Section 37. Feedback of Operating Experiences.....	21
<b>VI. INSPECTION AND ENFORCEMENT .....</b>	<b>21</b>
Section 38. Inspection.....	21
Section 39. Enforcement.....	21
Section 40. Violations.....	21
<b>VII. EFFECTIVITY .....</b>	<b>22</b>
Section 41. Effective Date.....	22
APPENDIX I. CATEGORIZATION OF NUCLEAR MATERIAL .....	23
APPENDIX II. FORMAT AND CONTENT OF TRANSPORT SECURITY PLAN .....	24
APPENDIX III. VULNERABILITY ASSESSMENT .....	33
APPENDIX IV. INTERNATIONAL TRANSPORT OF NUCLEAR MATERIAL .....	37



Republic of the Philippines  
Department of Science and Technology  
**PHILIPPINE NUCLEAR RESEARCH INSTITUTE**  
Commonwealth Avenue, Diliman, Quezon City

**CPR Part 32**

**SECURITY REQUIREMENTS IN THE TRANSPORT OF NUCLEAR MATERIAL**

**I. GENERAL PROVISIONS**

**Section 1. Purpose.**

- (a) The requirements of this Part are issued pursuant to Section 2 of Republic Act No. 5207, as amended, which provides as a matter of policy, to protect the public against the unauthorized use of nuclear material and associated activities.
- (b) The main objectives of the requirements of this Part are:
  - (1) To achieve and maintain a high level of security during transport of nuclear material that is commensurate with the potential risk posed by the material;
  - (2) To prevent unauthorized access or damage to, and loss, theft, or unauthorized transfer of nuclear material during transport; and
  - (3) To prevent unauthorized removal and sabotage during transport of nuclear material intended for malicious act.
- (c) The requirements of this Part shall be used in conjunction with other requirements of the Code of PNRI Regulations (CPR) covering licensing, nuclear safety and security and other regulatory controls relating to transport of nuclear material.
- (d) Nothing in this Part shall be construed to limit actions as may be appropriate and necessary to protect the health and safety of the radiation workers, general public and the environment as a consequence of a malicious act involving nuclear material.

**Section 2. Scope.**

- (a) The requirements in this Part shall apply to the security of nuclear material for protection against three types of malicious act:
  - (1) Unauthorized removal with the intent to construct a nuclear explosive device;

- (2) Unauthorized removal which could lead to subsequent dispersal; and
- (3) Sabotage
- (b) The requirements of this Part shall apply to the transport of nuclear material used for civil purposes in the Philippines by air, land or water, including loading, unloading, and in storage incidental to transport.
- (c) The requirements of this Part shall apply to actions to be undertaken by the licensee to locate and recover missing nuclear material.
- (d) Nothing in this Part relieves any person from complying with applicable requirements of other government agencies having jurisdiction over transport of nuclear material.

### **Section 3. *Specific Exemptions.***

PNRI may, upon application by a licensee or upon its own initiative, grant such exemptions from the requirements in this Part as it determines are authorized by the Act and are in the public interest, and will not endanger life, property and the environment nor compromise the national security and defense.

### **Section 4. *Definitions.***

As used in this Part:

- (a) **“Administrative Measures”** means the use of policies, procedures, instructions, sanctions, access control rules, confidentiality rules and techniques that direct personnel to securely and safely manage nuclear material;
- (b) **“Carrier”** means any person, including freight forwarders, engaged in the transport of nuclear material by land, air or water, as a common or contract carrier, or private entity;
- (c) **“CPR or Code”** means the Code of PNRI Regulations;
- (d) **“Consignee”** means any PNRI licensee who is entitled to take delivery of a consignment;
- (e) **“Consignment”** means any package or packages, or load of nuclear material, presented by a consignor for transport;
- (f) **“Consignor”** means any PNRI licensee who prepares a consignment for transport, or is named consignor in the transport documents;
- (g) **“Contingency plan”** means a predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts;
- (h) **“Conveyance”** means
  - (1) for transport by road or rail: any vehicle;
  - (2) for transport by water: any vessel, or any hold, compartment, or defined deck area of a vessel; and
  - (3) for transport by air: any aircraft.

- (i) **“Defence in depth”** means the combination of multiple layers of systems and measures that have to be overcome or circumvented before nuclear security is compromised;
- (j) **“Design basis threat”** means the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated;
- (k) **“Detection”** means 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.
- (l) **“Delay”** means security measures to impede or hinder the progress of an intruder;
- (m) **“Deterrence”** means security measures sufficient to deter a reasonable individual from attempting unauthorized access;
- (n) **“Diversion”** means the unauthorized movement of nuclear material subject to this Part to a location different from the material’s authorized destination inside or outside of the site at which the material is used or stored;
- (o) **“Export”** means the physical transfer of one or more nuclear material covered by this Part originating from the Philippines into an importing state, or to a recipient in an importing state;
- (p) **“Graded approach”** means the application of nuclear security measures proportionate to the potential consequences of a malicious act
- (q) **“Import”** means the physical transfer of one or more nuclear material covered by this Part, into the Philippines or to a recipient in the Philippines and originating from an exporting state;
- (r) **“Licensee”** means a holder of a valid license issued by PNRI;
- (s) **“Law Enforcement Agency (LEA)”** means the agency that has authority to carry firearms and make arrests, and is authorized and has the capability to provide an armed response in the jurisdiction where the licensed nuclear material is transported or in in-transit storage;
- (t) **“Malicious Act”** means a deliberate act to remove nuclear material from authorized control or an act directed against nuclear material that could endanger workers, the public and the environment by exposure to radiation or the release or dispersal of nuclear material, including the deliberate dispersion of nuclear material to cause economic and social disruption;
- (u) **“Nuclear material”** means plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; uranium enriched in the isotope 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore residue; any material containing one or more of the foregoing;
- (v) **“Nuclear Security”** means the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities;

- (w) **“Nuclear security culture”** means the assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serves as a means to support, enhance and sustain nuclear security;
- (x) **“Nuclear security event”** means an event that has potential or actual implications for nuclear security that must be addressed;
- (y) **“Performance Testing”** means testing of the physical protection measures and the physical protection system to determine whether or not they are: implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements;
- (z) **“Physical Protection Measures”** means the personnel, procedures and equipment that constitute a physical protection system;
- (aa) **“Physical Protection System”** means an integrated set of physical protection measures intended to prevent the completion of a malicious act;
- (bb) **“Readiness Review”** means a systematic review carried out by a licensee prior to undertaking a shipment as part of a good security management program to ensure overall functioning of a security system. A readiness review is used to demonstrate that security measures are in place and functional prior to starting shipment operations;
- (cc) **“Response Force”** means persons, on-site or off-site who are qualified, authorized, and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage;
- (dd) **“Risk”** means a multiattribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with exposures or potential exposures;
- (ee) **“Risk Assessment”** means assessment of the radiation risks and other risks associated with normal operation and possible accidents involving facilities and activities;
- (ff) **“Sabotage”** means a deliberate act directed against nuclear material during transport or in-transit storage that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of nuclear material;
- (gg) **“Security Manager”** means a person duly designated by the licensee as the point of contact for the implementation of security requirements;
- (hh) **“Security System”** means a system designed by the licensee which satisfies the requirements specified in the requirements of this Part as documented in the Transport Security Plan;
- (ii) **“Shipment”** means the specific movement of a consignment from origin to destination;
- (jj) **“Storage”** means the interim holding of nuclear material incidental to transport;
- (kk) **“Threat”** means a characterization of an adversary capable of causing undesirable consequences, including the objectives, motivation and capabilities, e.g. number of potential attackers, equipment, training and attack plan;

- (ll) **“Threat Assessment”** means an analysis that documents the credible motivations, intentions and capabilities of potential adversaries that could cause undesirable consequences with regard to nuclear material in transport;
- (mm) **“Transport Control Center (TCC)”** means an operations center that is remote from transport activity and that maintains continuous conveyance location and security status information for a shipment of nuclear material;
- (nn) **“Transport Security Plan (TSP)”** means a document prepared by the licensee that presents a detailed description of the security arrangements during transport of nuclear material;
- (oo) **“Trustworthiness”** means the characteristics of an individual considered dependable in judgment, character and performance, such that unescorted access to nuclear material by that individual does not constitute an unreasonable risk to the public health and safety or security. A determination of trustworthiness for this purpose is based upon the results from a background investigation;
- (pp) **“Unescorted Access”** means solitary access to packages or the devices that contain the material including unescorted access to the cargo area of a conveyance; and
- (qq) **“Worker”** means any individual engaged full time or part time in the transport of nuclear material.

## **Section 5. Interpretation.**

Except as specifically authorized by PNRI in writing, no interpretation of the meaning of the requirements in this Part by any officer or employee of PNRI other than a written interpretation by the Director, will be recognized to be binding upon the PNRI.

## **Section 6. General Obligations.**

No person shall engage in the transport of nuclear material except as authorized by a license issued by PNRI pursuant to a specific regulation of the CPR and unless the requirements of this Part are complied with.

## **Section 7. Access to Premises and Information.**

For purposes of implementing its licensing and regulatory functions pursuant to the Act, authorized representatives of PNRI, in coordination with other relevant regulatory agencies, may access premises, facilities and conveyances used in the transport of nuclear material subject to this Part in order to obtain information about the status of security and verify compliance with regulatory requirements.

## **Section 8. Resolution of Conflicts.**

PNRI may initiate the appropriate steps toward the resolution of a conflict, if any, between the requirements contained in this Part and other laws and regulations.

**Section 9. *Additional Requirements.***

PNRI may impose additional requirements by regulation, administrative order, or conditions of a license, in addition to those established in this Part, as it deems appropriate or necessary to protect health and safety of radiation workers, the general public and the environment, and will not endanger property nor compromise the national security and defense.

**Section 10. *Transport Requirements Addressed by Other National Modal Agencies.***

PNRI may apply, as may be practicable, specific provisions of the International Maritime Dangerous Goods (IMDG) Code, Safety of Life at Sea (SOLAS), International Civil Aviation Organization (ICAO) Technical Instructions, International Ship and Ports Facility Security (ISPS) Code, and relevant requirements adopted by other national modal agencies on transport, including the Office for Transportation Security National Transport Security Program (OTS NTSP).

**Section 11. *Communication.***

All communications and reports concerning the requirements of this Part shall be addressed to the Director, Philippine Nuclear Research Institute (PNRI), Commonwealth Avenue, Diliman, Quezon City.

**II. ADMINISTRATIVE REQUIREMENTS**

**Section 12. *Responsibilities of the Licensee.***

- (a) The licensee shall establish and implement the administrative and technical measures that are needed to ensure the security of nuclear material during transport and to comply with all applicable requirements of this Part and the conditions of the license.
- (b) The licensee shall bear full responsibility for the actions of any organization that may be contracted to undertake transport operations on its behalf. The licensee shall:
  - (1) Identify all workers whose assigned tasks could substantially affect the security of nuclear material during transport;
  - (2) Ensure that workers authorized by reference in the license are permitted to fulfill required assignments and tasks;
  - (3) Ensure that workers meet the requirements for training and trustworthiness as specified in this Part;
  - (4) Notify PNRI of its intention to introduce any change in the transport arrangements which could have implications to security; and
- (c) The licensee shall designate a Security Manager in key assignments related to the security in the transport of nuclear material.



**Section 13. Security Manager.**

- (a) The Security Manager shall be responsible for the development and implementation of the Transport Security Plan (TSP).
- (b) The Security Manager shall provide analysis and advice to ensure that security requirements are being implemented in a manner that does not compromise safety.
- (c) The Security Manager shall coordinate with the licensee's Radiation Protection Officer in matters related to radiation safety during transport of nuclear material.
- (d) The Security Manager shall be the single point of contact responsible for all security related actions during the actual transport of nuclear material.

**Section 14. Security Culture.**

The licensee shall promote security culture and establish a management system, commensurate with the size and nature of the transport operation, which ensures that:

- (a) Policies and procedures are established that identify security, along with safety, as being of the highest priority;
- (b) Problems affecting security are promptly identified and corrected in a manner commensurate with their importance;
- (c) The responsibilities of each individual for security are clearly identified and each individual is suitably trained and qualified;
- (d) Clear lines of authority for decisions on security are defined;
- (e) Organizational arrangements and lines of communications are established that result in an appropriate flow of information on security at, and between, the various levels in the entire organization of the licensee, and other concerned parties; and
- (f) Sensitive information relative to the security of the nuclear material is identified and protected according to this Part and other applicable Philippine law.

**Section 15. Personnel Access Authorization.**

- (a) The licensee shall subject the following individuals to access authorization measures:
  - (1) Individuals whose assigned duties require unescorted access to the packages or devices containing nuclear material;
  - (2) Individuals whose assigned duties require access to the packages or devices containing nuclear material;
  - (3) Licensee personnel transporting the nuclear material, if the licensee transports its own nuclear material;
  - (4) Vehicle drivers and accompanying individuals, for road shipments; and
  - (5) Individuals assigned to man the Transport Control Center (TCC).

- (b) The licensee shall grant unescorted access to the packages or devices containing nuclear material only to individuals determined to be trustworthy as defined in Section 17 of this Part.
- (c) The licensee shall ensure that the requirements in Section 24 of this Part are met.

**Section 16. Confidentiality and Information Security.**

- (a) The licensee shall establish an information management system, commensurate with the category of nuclear material involved in the transport operation, which ensures that the:
  - (1) Confidentiality of information that it receives in confidence from another party is protected;
  - (2) Information received in confidence from another party is only provided to a third party with the consent of the first party; and
  - (3) Confidentiality of information, the unauthorized disclosure of which could compromise the effectiveness of the transport security system.
  - (4) Critical systems and sensitive information are protected from cyber threats.
- (b) Information and documents that can be used to identify transport routes, schedules, specific security measures or weaknesses in the transport security system shall be controlled and distributed only on a need-to-know basis. These information and documents include:
  - (1) Specific routes, shipment schedules, and in-transit storage locations;
  - (2) Transport Security Plan, if applicable and associated documents;
  - (3) Transport security system and associated documents;
  - (4) Temporary or permanent weaknesses in the security system; and
  - (5) Transport emergency response and contingency plan.

**Section 17. Trustworthiness of Individuals Involved in Transport Operation.**

- (a) The licensee shall take measures to determine the trustworthiness of the following:
  - (1) Individuals specified in Section 15 of this Part; and
  - (2) Individuals requiring access to the security sensitive information specified in Section 16 of this Part.
- (b) The licensee shall conduct appropriate background checks and psychological examinations from accredited institutions to the individuals identified in (a).
- (c) The measures to determine trustworthiness shall be commensurate with the category of nuclear material applicable to the transport operation.

**Section 18. *Training Requirements.***

- (a) The licensee shall ensure that workers, commensurate with responsibilities and roles and on a need-to-know basis:
  - (1) Are instructed in the licensee's TSP and implementing procedures, the responsibilities, and the appropriate response to security incidents;
  - (2) Receive training on security awareness that addresses the nature of security related threats and includes:
    - (i) the TSP;
    - (ii) emergency response and contingency plan; and
    - (iii) other associated plans.
- (b) The licensee with dedicated security personnel shall train the security personnel in the timely notification of affected Law Enforcement Agency (LEA) during emergencies.
- (c) Personnel subject to the training requirements of this Part shall complete the training before being allowed unescorted access to nuclear material.
- (d) The licensee shall require workers to undertake annual retraining. The retraining shall address:
  - (1) Any significant change in the TSP;
  - (2) Reports on relevant threats, problems or lessons learned;
  - (3) Relevant results from readiness reviews and inspections by PNRI or other responsible groups or organizations; and
  - (4) Relevant results from the licensee's own reviews and evaluations.
- (e) Training records shall be maintained for three (3) years and shall include training topics, training dates, and the list of personnel who attended the training.

**Section 19. *Transport Control Center (TCC).***

The licensee transporting a Category I and II nuclear material shall establish a Transport Control Center (TCC) or other central point of communication to:

- (a) monitor and coordinate voice and/or digital communications between personnel involved with a specific shipment or group of shipments;
- (b) monitor positional tracking;
- (c) facilitate command; and
- (d) ensure effective coordination with the emergency response.

**Section 20. *Performance Testing and Verification of Compliance.***

The licensee who regularly undertakes transport operation shall conduct performance testing of transport security systems to verify compliance with the requirements of this Part and the conditions of the license. Testing shall include drills and exercises in which personnel exhibit their understanding and ability to perform their required tasks annually or as deemed necessary by PNRI.

### III. TECHNICAL REQUIREMENTS

#### **Section 21. *Graded Approach.***

- (a) Physical protection measures shall be based on a graded approach, considering the current assessment of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material.
- (b) The licensee shall implement the graded approach on the basis of categorization of nuclear material as described in APPENDIX I, Categorization of Nuclear Material.
- (c) The licensee shall use the total amount of nuclear material on or in a single conveyance to determine an aggregate categorization for both unauthorized removal and potential radiological consequences associated with sabotage and identify the appropriate protection measures for the conveyance. When different types of nuclear materials are transported on the same conveyance, the aggregation formula established by the PNRI shall be used to determine the category of the consignment.
- (d) The licensee shall ensure that the physical protection measures for detection, delay and response are based on the principle of defence in depth applied with a graded approach.

#### **Section 22. *Contingency Plan.***

- (a) The licensee shall develop contingency plans for the location and rapid recovery of nuclear material which has been declared missing or stolen during transport.
- (b) Contingency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear material during transport, or attempts thereof, shall be prepared, and appropriately exercised periodically by the licensees.

#### **Section 23. *Physical Protection Program.***

- (a) The licensee shall develop and maintain a physical protection program approved by the PNRI according to the format and content specified by the PNRI.
- (b) The licensee's physical protection program shall include:
  - (1) Transport Security Plan;

- (2) Security Measures;
  - (3) Contingency Plan;
  - (4) Training and Re-training Plan; and
  - (5) Implementing Procedures.
- (c) The licensee shall ensure the implementation of an approved physical protection program through drills and exercises.
- (d) The licensee shall implement physical protection measures for nuclear material based on the material's category.

**Section 24. *Review and Evaluation.***

- (a) The licensee shall review the physical protection program annually by individuals independent of both physical protection program management and personnel who have direct responsibility for implementation.
- (b) Review of the physical protection program shall include, but not be limited to, an audit of the effectiveness of the physical protection program, relevant plans, implementing procedures, safety and physical protection interface activities, the testing, maintenance, and calibration program.
- (c) The outcome of the physical protection program review, and any actions taken as a result of prior reviews, shall be documented and reports shall be maintained in an auditable form.
- (d) Evaluations, including performance testing of physical protection measures and of the integrated physical protection system, including timely response of the guards and response forces shall be conducted regularly to determine the reliability and effectiveness against the threat.
- (e) Performance testing of physical protection system shall include transport security exercises to determine if the response forces can provide an effective and timely response to prevent malicious act.

**Section 25. *Transport Security Plan.***

- (a) A transport security plan shall be developed by the licensee for Category I and II nuclear material.
- (b) The transport security plan may be developed by the shipper and/or the carrier.
- (c) The transport security plan shall be tested or evaluated as appropriate and evaluated and updated at least once a year or as deemed necessary by PNRI.
- (d) Identified deficiencies in the transport security plan or security systems shall be promptly remedied and reported in accordance with Section 35 of this Part.

- (e) The licensee shall retain a copy of the current transport security plan as a record until PNRI terminates the license and, if any portion of the plan is superseded, retain the superseded material for five (5) years.

#### **IV. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT**

##### **Section 26. *General Requirements.***

- (a) The licensee shall implement the following measures in accordance with the graded approach:
  - (1) Minimizing the total time during which the nuclear material remains in transport;
  - (2) Minimizing the number of transfers and duration of transport of nuclear material;
  - (3) Protecting nuclear material during transport and in temporary storage facility in a manner consistent with the applicable category of that nuclear material;
  - (4) Avoiding the use of predictable movement schedules by varying times and routes;
  - (5) Requiring predetermination of the trustworthiness of individuals involved during transport of nuclear material;
  - (6) Limiting advance knowledge of transport information to the minimum number of persons necessary;
  - (7) Use a conveyance with passive and/or active physical protection measures appropriate for the threat assessment or design basis threat;
  - (8) Using routes which avoid areas of natural disaster, civil disorder or known threat; and
  - (9) Ensuring that packages and/or conveyances are not left unattended for any longer than is absolutely necessary.

##### **Section 27. *Requirements for Category I, II and III Nuclear Material.***

In addition to the general requirements given in Section 26 of this Part, the following requirements also apply to apply to Categories I, II and III nuclear material:

- (a) The carrier shall give the receiver advance notification of the planned shipment specifying the mode of transport, the estimated time of arrival of the shipment and the exact point of handover 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.

- (b) The licensee shall ensure that prior agreements among consignor, consignee, and carrier specify the time, place and procedures for transferring physical protection responsibilities.
- (c) Locks and seals shall be applied to conveyances, compartments or freight containers. If locks and/or seals are used, checks shall be made before dispatch and during any intermodal transfer of each nuclear material consignment to confirm the integrity of the locks and seals on the package, vehicle, compartment or freight container.
- (d) Packages containing nuclear material shall 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 shall be tied down or attached to the vehicle or freight container and should be secured as appropriate.
- (e) The consignor or carrier shall provide consignment specific transport documents to appropriate carrier personnel. Drivers or operators of all conveyances used shall be given emergency contact information for the areas through which they will be passing. The information may be part of other instructions or manuals, such as shipboard emergency procedures. The documents shall be provided in the languages deemed necessary by the shipper, carrier or the authorities concerned and any confidentiality requirements shall be followed.
- (f) There shall be a detailed search of 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.
- (g) Consideration shall be given to using a method for periodically identifying the location of a shipment of nuclear material. Information concerning the location of the shipment shall be properly controlled but shall be readily available to the shipper and/or carrier, and shall be provided to the receiver when appropriate.
- (h) Arrangements shall be made to provide sufficient response forces to deal with nuclear security events consistent with the category of nuclear material being transported and physical protection measures shall include communication from the conveyance capable of summoning appropriate responders.
- (i) The shipper and carrier shall maintain and have readily available, to the extent possible, accurate information on how to summon local response forces close to the route being used.
- (j) The receiver shall check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver shall notify the shipper of the arrival of the shipment immediately or of nonarrival within a reasonable interval after the estimated time of arrival at the destination.

**Section 28. Requirements for Category I and II Nuclear Material.**

In addition to the general requirements prescribed in Section 26 and specific requirements in Section 27 of this Part, the following requirements also apply to Category I and II nuclear material:

- (a) The receiver shall confirm readiness to accept delivery and handover, if applicable, at the expected time, prior to the commencement of the shipment.
- (b) Selection of transport mode and routing:
  - (1) A transport security plan shall be submitted by the consignor as appropriate to the PNRI for approval. A plan may cover a series of similar movements. This plan shall address routing of the shipment, stopping places, destination hand-over arrangements, identification of persons authorized to take delivery, accident procedures, reporting procedures, both routine and emergency, and as appropriate, contingency plans. In choosing the route, the capabilities of the response forces should be taken into account.
  - (2) Exercises shall be conducted by the consignor to assess and validate the transport security plan and to train the participants on how to respond to nuclear security events.
  - (3) Prior to commencing transport, the licensee shall ensure that all measures necessary to implement the approved transport security plan are in place.
- (c) The conveyance shall be searched immediately prior to loading and shipment. Immediately following completion of the search, the conveyance shall be placed in a secure area or kept under guard surveillance until its loading and shipment for transport and unloading.
- (d) Personnel with physical protection responsibilities shall be given written instructions that, when appropriate, have been approved by the PNRI, detailing their responsibilities during the transport.
- (e) The physical protection measures applied to the conveyance, freight container and package shall include delay measures to increase the time required by an adversary to complete the unauthorized removal of the nuclear material. The delay should be sufficient so that guards and response forces have reasonable time to make an appropriate response.
- (f) High strength and high security locks shall be required.
- (g) The licensee shall ensure that appropriately equipped and trained guards shall accompany each shipment, including before and during loading and unloading operations.
- (h) The licensee shall use method of providing continuous tracking of the location of shipment of nuclear material.
- (i) A transport control center (TCC), as the central point of communication, shall be established to monitor and coordinate voice and digital communications between



personnel involved with the shipment, to monitor positional tracking, and to facilitate command and control.

- (j) Physical protection measures shall include provision of continuous two-way voice communication systems between the conveyance, any guards accompanying the shipment, the designated response forces, and where appropriate, the shipper and receiver.
- (k) The licensee shall make arrangements for the availability of response forces proportional to the prevailing threat to deal with nuclear security events in time to prevent the unauthorized removal of nuclear material.
- (l) Depending on the mode of transport, the consignment shall be shipped by:
  - (1) Road, under exclusive use conditions; or
  - (2) Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked conveyance; or
  - (3) Water, in a secure compartment or container which is locked and sealed; or
  - (4) Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.
- (m) While nuclear material is on board pending departure, provisions shall be made for sufficient access delay or compensating measures to meet the threat assessment or design basis threat.

**Section 29. *Requirements for Category I Nuclear Material.***

- (a) In addition to the general requirements prescribed in Section 26 and specific requirements in Section 27 and 28 of this Part, the following requirements also apply to Category I nuclear material:
  - (1) The approval by the PNRI of the transport security plan shall be based on a detailed examination of proposed physical protection measures, which shall provide sufficient delay so that guards and/or response forces have time to intervene to prevent unauthorized removal. The transport security plan shall include the route and arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, threat assessment and operating conditions.
  - (2) A further authorization by the competent authority of the shipment shall be required just prior to commencing transport and shall be conditional on a current threat assessment and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment.

- (3) Engineered alarm or intrusion detection systems shall be applied to conveyances to the extent practicable. These systems shall be redundant, and capable of being monitored from the transport control center.
- (4) When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, enhanced physical protection measures shall be applied, such as additional guards. The package shall be tied down or attached to the conveyance or freight container with multiple locking mechanisms that require two different keys to be unlocked held by two different authorized persons. The locking devices should not interfere with the safety performance of the package.
- (5) Security inspections shall be performed on all equipment, stores, personal effects and other goods loaded onto the conveyance.
- (6) Guards providing surveillance shall do so under conditions which ensure close communication with response forces.
- (7) The licensee shall establish a transport control center 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 center shall be protected so that its function can continue in the presence of the threat. While the shipment is in progress, the transport control center shall be staffed by appropriate personnel whose trustworthiness has been predetermined
- (8) The licensee shall maintain continuous two-way communication systems between the conveyance, transport control center, guards accompanying the shipment, the designated response forces, and where appropriate, the shipper and/or receiver shall be redundant, diverse and secure.
- (9) Prior Shipment Requirements:
  - (i) The PNRI shall be informed about exact date and time of shipment prior to the commencement of each shipment.
  - (ii) A detailed route surveillance shall be conducted based on the threat assessment or intelligence information.
- (10) 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. 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 should carry a guard or crew member in addition to the driver. 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.

- (11) During shipment by rail, accompanying guards should travel close to the conveyance to have proper effective surveillance.
- (12) For shipments by water, the consignment shall be transported in a dedicated transport vessel. Security personnel should search:
  - (i) All personal items as they are brought on board the ship;
  - (ii) All persons entering the secure area; and
  - (iii) All stores for the voyage as they are brought on board the ship.

Prior to commencing loading of the shipment, security personnel should also search:

- (i) Dockside areas adjacent to the ship;
- (ii) Compartments adjacent to that containing the nuclear material;
- (iii) The whole ship, including stores and the engine room; and
- (iv) The underwater section of the ship's hull.

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

- (13) Critically sensitive areas and systems, such as the engine room, navigation bridge, communications areas and guards' positions, shall be secured with limited access and shall be kept locked at all times during transport.
- (14) The ship shall have a hardened control room for the purpose of command and control of the guards. The control room shall be staffed by the guards' command staff and, where possible, be in a location near the center line of the ship with other compartments around it to prevent disablement of the control room by attack from outside the ship, and delay any attack from within the ship.
- (15) Guards shall accompany the maritime shipment on the load carrying ship and/or on an accompanying ship in a location where they can best respond to an attack, in accordance with the information provided in the TSP. Guards shall be able to communicate with the captain and bridge as well as the transport control center, and should be capable of activating any active detection and communication systems, the features of which should be clearly defined in the TSP.

- (16) Consideration shall be given to providing the load carrying ship with the means that will allow the crew and the guards to be aware of any ship or aircraft that might be approaching, particularly on the high seas.
- (17) Ports of call along the route shall be avoided.
- (18) To prevent tampering and protect information on the design of the physical protection equipment, the ship should be protected from unauthorized access or observation even when it is not occupied.
- (19) For shipments by air, the consignment shall be transported in an aircraft designated for cargo only and for which the nuclear material is its sole cargo.

**Section 30. *Nuclear Material that Poses Radiological Risk.***

- (a) For some nuclear material falling under Category III and below Category III, prudent management practices of physical protection shall include the following:
  - (1) Basic security awareness training for all personnel involved;
  - (2) Verification of the identity of all personnel involved;
  - (3) Verification of security of conveyances used;
  - (4) Availability of written instructions;
  - (5) Exchange of information on security measures between operators, shippers or carriers and with competent authorities ensuring the need for confidentiality; and
  - (6) Determining the trustworthiness of the personnel involved.

**Section 31. *Measures to Locate and Recover Missing or Stolen Nuclear Material during Transport.***

- (a) The licensee shall be alert during transport for any indications that packages have been removed from conveyance or tampered with and shall verify during delivery that no packages are missing or have been tampered.
- (b) The licensee shall take immediate action to determine if missing packages are misplaced but still under its control.
- (c) The licensee shall immediately report to the PNRI if packages are determined to be missing or have been tampered with.
- (d) The licensee shall assist and coordinate with the response organizations to locate and recover its missing or unauthorizedly removed nuclear material.

**Section 32. *Measures for Protection against Sabotage.***

- (a) The licensee shall prepare transport personnel to act in full coordination with guards, response forces and law enforcement agencies for implementing the contingency plan.
- (b) The transport control center or carrier's management shall be informed as soon as an attempt or an act of sabotage is detected.
- (c) The licensee shall notify immediately, the shipper, the PNRI, response forces and other relevant government agencies of sabotage or attempted sabotage as specified in the contingency plan.
- (d) Immediately following an act of sabotage, the carrier and/or guards shall take measures to secure the transport and minimize the consequences of the act.

**Section 33. *Measures to Mitigate or Minimize the Radiological Consequences of Sabotage.***

- (a) The licensee shall assess, on detection of a malicious act, whether this act could lead to radiological consequences and notify the PNRI.
- (b) Immediately following an act of sabotage, the licensee shall take measures specified in the contingency plan to prevent further damage.

**V. RECORDING AND REPORTING REQUIREMENTS**

**Section 34. *Inventories and Records.***

- (a) Nuclear material shall be inventoried and accounted for before and after shipment, and additionally, if applicable, at regular intervals during in-transit storage, depending on the length of storage.
- (b) The licensee shall maintain records of the following:
  - (1) Transport security plan;
  - (2) Readiness reviews;
  - (3) Inventories;
  - (4) Emergency exercises, including drills;
  - (5) Advance notifications;
  - (6) Revision or cancellation notices, if any;
  - (7) Correspondence related to transport of nuclear material;
  - (8) Copies of transport documents, including documentation of receipt or non-receipt; and
  - (9) Event/incident reports.
- (c) The licensee shall maintain safeguards against tampering with and loss of records.

- (d) Signed and authenticated records required by this Part shall be retained for a period of three (3) years, kept legible throughout the retention period, and made available for PNRI inspection, upon reasonable notification.

**Section 35. Reporting Requirements.**

- (a) In addition to any reporting required by the other relevant Parts of the CPR, the licensee shall make the following reports to PNRI:
  - (1) Inventory data as specified in Section 34(a) of this Part;
  - (2) Unusual events or incidents, such as:
    - (i) failures of transport packaging or containers, which may have security implications,
    - (ii) discovery of any unaccounted nuclear material,
    - (iii) unauthorized access to the nuclear material,
    - (iv) loss of control over the nuclear material,
    - (v) actual or attempted theft or sabotage of nuclear material, and
    - (vi) receipt of specific or general malicious threats;
  - (3) Identified security system vulnerabilities and corrective actions taken; and
  - (4) Any intentions to introduce modifications to any transport arrangement whenever the modifications could have significant implications for security.
- (b) Any event or incident specified in Section 35(a)(2) above shall be reported in writing within a period of ten (10) working days following proper notification according to Section 36 of this Part.
- (c) All other reports required by this Part shall be made in writing within a period of thirty (30) days.

**Section 36. Notification of Incidents.**

- (a) The licensee shall notify PNRI within twenty-four (24) hours by an appropriate method of any events or incidents specified in Section 36(a)(2)(i) through (iii) of this Part.
- (b) The licensee shall notify both the LEA and PNRI of events or incidents specified in Section 36(a)(2)(iv) through (vi) of this Part as follows:
  - (1) The licensee shall immediately notify the LEA, through telephone, after determining that an unauthorized access resulted in an actual or attempted theft, sabotage or diversion of a nuclear material or situations that pose a potential risk to the health and safety of the general public and the environment. The licensee shall notify PNRI as soon as possible after initiating a response, but not at the expense of causing delay or interfering with the LEA response to the event; and
  - (2) The licensee shall immediately notify the LEA, through telephone, any suspicious activity related to possible theft, sabotage or diversion of nuclear material. The licensee shall notify PNRI as soon as possible after notifying the LEA.

- (c) The initial notifications required in Section 36(a) and (b) above shall be followed within a period of ten (10) working days by a written report submitted to PNRI by an appropriate method in accordance with Section 36 of this Part. The report must include sufficient information for PNRI assessment and evaluation, including identification of any necessary corrective actions to prevent future instances.

**Section 37. *Feedback of Operating Experiences.***

The licensee shall ensure that information on normal operational performance, abnormal conditions, and events that may affect the security of nuclear material during transport, including best practices and deficiencies identified during the transport operations, is made available to PNRI.

**VI. INSPECTION AND ENFORCEMENT**

**Section 38. *Inspection.***

- (a) The licensee shall afford PNRI the opportunity to conduct inspection of transport security measures implemented.
- (b) The licensee shall be made available to PNRI for inspection records specified in Section 35 of this Part pertaining to the shipment of nuclear material.

**Section 39. *Enforcement.***

In case of any non-compliance of these requirements, enforcement action will be initiated by the PNRI.

**Section 40. *Violations.***

- (a) A notice of violation shall be issued to the licensee who may be found to have violated the requirements of this Part, or any order or rule issued hereunder.
- (b) PNRI may revoke, suspend or modify a license to use nuclear material, or prohibit the possession of nuclear material, upon finding a lapse in the security of nuclear material during transport or non-compliance with applicable requirements of this Part.
- (c) Any person who willfully violates, attempts to violate, or conspires to violate, any provision of this Part, rule or order issued pursuant to this Part, may be guilty of a crime, and upon conviction, may be punished by a fine or imprisonment, or both, as provided by Sections 64 and 65 of Republic Act No. 5207.

## VII. EFFECTIVITY

### Section 41. *Effective Date.*

The requirements of this Part shall take effect fifteen (15) days following the publication of this Part in the Official Gazette.

**APPROVED:**



**CARLO A. ARCILLA, Ph.D.**  
Director, PNRI

Date: 15 November 2024



**APPENDIX I. CATEGORIZATION OF NUCLEAR MATERIAL**

Material	Form	Category		
		Category I	Category II	Category III <sup>a</sup>
1. Plutonium <sup>b</sup>	Unirradiated <sup>c</sup>	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (235U)	Unirradiated <sup>c</sup> – Uranium enriched to 20% 235U or more – Uranium enriched to 10% 235U but less than 20% 235U – Uranium enriched above natural, but less than 10% 235U	5 kg or more	Less than 5 kg but more than 1 kg  10 kg or more	1 kg or less but more than 15 g  Less than 10kg but more than 1 kg  10 kg or more
3. Uranium-233 (233U)	Unirradiated <sup>c</sup>	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (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.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content) <sup>d,e</sup>	

<sup>a</sup>Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

<sup>b</sup>All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

<sup>c</sup>Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h. (100 rad/h) at 1 m unshielded.

<sup>d</sup>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.

<sup>e</sup>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/h (100 rad/h) at one meter unshielded.

## **APPENDIX II.       FORMAT AND CONTENT OF TRANSPORT SECURITY PLAN**

- (1) An example structure of a transport security plan (TSP) for use is provided in Box 1. A State may need to modify this outline to reflect its own particular circumstances, but the example contains all of the information that the State needs in order to validate and approve the transport activities of those who propose to transport nuclear material. States should require this structure or a structure similar to this to facilitate understanding between shippers, carriers, receivers and regulators, both domestically and internationally.
- (2) For information security reasons, the PNRI may require that the TSP be developed in the form of a series of separate documents, each of which may be provided only to those that need to know those parts of the plan.
- (3) In addition, the entity responsible for preparing and submitting the TSP has access to knowledge from the Philippines' threat assessments or DBT, enhanced protection of the information in the TSP or elements thereof may be needed.
- (4) For the prescriptive approach, the listing of provisions required by the PNRI should be inserted in section 1.2.2 of the example structure in Box 1.
- (5) The following sections outline the details that should be considered for inclusion in a TSP for a shipment undertaken following the performance based approach. If the entity responsible for preparing and submitting the TSP is required by the competent authorities to apply the performance based or combined approach, a vulnerability assessment may be required.

### **ADMINISTRATIVE REQUIREMENTS AND INFORMATION**

- (6) This section should include the complete legal name and address of the entity responsible for preparing and submitting the TSP, plus all appropriate telephone, fax and email addresses of those who are applying for approval of the TSP. This should include information about the shipper, carriers or others who might be involved with the proposed shipment, including guards employed for the shipment, and information about the receiver and transit States when international transport is proposed. It should also contain detailed information in subsections as elaborated in the following.

#### **Allocation of responsibilities**

- (7) The TSP should clearly establish responsibility for each of the provisions and measures specified therein. It should identify all involved personnel who have the appropriate authority to carry out their responsibilities, and should clearly specify who — the shipper, carrier or receiver — has direct responsibility for the security of the nuclear material during each particular mode or phase of the transport. Whenever responsibility for a shipment is to be changed from one party to another (e.g. between carriers at a national border, or between a carrier or receiver, or a facility operator when the shipment is being placed into in-transit storage), the transfer of responsibilities should be specified.
- (8) If any transport activities are subcontracted, the TSP should identify all contractual arrangements that will be needed to develop and comply with the TSP.

**BOX 1: EXAMPLE STRUCTURE OF THE TRANSPORT SECURITY  
PLAN FOR THE PERFORMANCE BASED APPROACH**

**1. ADMINISTRATIVE REQUIREMENTS AND INFORMATION**

- 1.1. Allocation of responsibilities
- 1.2. Policies and operational procedures
  - 1.2.1. Vulnerability assessment
  - 1.2.2. Testing and evaluation of the transport security plan
  - 1.2.3. Review and update of the transport security plan
  - 1.2.4. Response to higher threat conditions
  - 1.2.5. Reporting of threats or incidents
- 1.3. Training requirements
- 1.4. Information management
  - 1.4.1. Retention of records
  - 1.4.2. Confidentiality and protection of information
- 1.5. Trustworthiness of personnel

**2. SHIPMENT SECURITY**

- 2.1. Description of the nuclear material to be transported
- 2.2. Description of the transport physical protection system
  - 2.2.1. Packages and conveyances
  - 2.2.2. Planned and alternative routes and modes of transport
  - 2.2.3. Physical protection measures
  - 2.2.4. Communications and positional tracking for normal operations
  - 2.2.5. Command and control for normal operations
- 2.3. Maintenance and testing of systems and equipment
- 2.4. Pre-shipment checks

**3. RESPONSE PLANNING**

- 3.1. Emergency arrangements
- 3.2. Contingency plans
  - 3.2.1. Guards
  - 3.2.2. Response forces
- 3.3. Incident communications, command and control

TSP to prepare a vulnerability assessment. Testing and evaluation of the transport security plan

- (9) Relevant policies and operational procedures should be clearly documented in this section of the TSP, including detailed measures to implement policies (e.g. policies on response procedures for higher threat conditions and employment verification for new staff), operating practices (e.g. choice and use of routes where known, use of guards and access to nuclear material packages at temporary storage facilities en route), and equipment and resources that are to be used to reduce security risks.

### **Vulnerability assessment**

- (10) For the performance based approach, and some variants of the combined approach, the administrative and technical requirements specified in the regulation should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment. The PNRI may require the entity responsible for preparing and submitting the Policies and operational procedures
- (11) The TSP should specify the procedures for evaluating and testing it. Review and update of the transport security plan
- (12) The TSP should be reviewed periodically, and updated when necessary, to ensure that the latest information available to the State relevant to the security of nuclear material shipments is taken into account. The TSP should specify when and how such reviews and updates are to be conducted. Response to higher threat conditions
- (13) As required by the PNRI, the TSP should be evaluated periodically to ensure that the most recent threat information is taken into account. Should the State designate that a higher threat condition exists at the time the shipment is to be undertaken than was assumed in developing the current TSP, appropriate actions should be taken to address this higher threat condition and a revised TSP should be developed.

### **Reporting of threats or incidents**

- (14) The TSP should require that any incidents or unscheduled delays that occur during transport be documented by the carrier and reported, within a specified time, to the shipper, receiver and, if applicable, the competent authorities. The TSP should also specify that a review of physical protection arrangements should be undertaken after a shipment is completed in order to evaluate the effectiveness of the TSP and to identify any necessary improvements which may be made to improve its effectiveness for future shipments.

### **Training requirements**

- (15) This section of the TSP should identify the training that will be conducted and the exercises that will be arranged, and specify the schedule that will be followed for each (since the State competent authorities or equivalent bodies may wish to witness the exercises). The training and exercises should address all appropriate aspects of physical protection, including for the management of organizational interfaces and specified functions for emergency response. Arrangements should be made for the results of exercises to be systematically evaluated by the participating organizations and, as appropriate, by the appropriate State competent authority. The results of all training exercises should be documented, and any corrective actions identified during the process should be implemented promptly.

### **Information management**

- (16) The TSP should clearly define the measures to be taken to protect the confidentiality of information deemed sensitive or classified by the competent authorities. Information management procedures should ensure that the distribution of sensitive transport information is limited to appropriate individuals on a need to know basis. Such measures should not preclude the proper application of provisions needed in transport documents and shippers' declarations as required by the IAEA Transport Regulations.

### **Retention of records**

- (17) This section of the TSP should address how the records of nuclear material shipments, including details of the packages used and the nuclear material they contained, and information on the personnel involved in the shipment, should be maintained and updated as necessary, consistent with requirements specified by the competent authorities. In addition, records should be maintained of all nuclear material that has been transported through the State. Records associated with the preparation and actual undertaking of a shipment, including the training and qualification of personnel, should be retained in a manner and for a time period that is consistent with that specified by the State.

### **Confidentiality and protection of information**

- (18) This section of the TSP should describe measures to be taken, consistent with national requirements, to protect the confidentiality of information relating to transport operations. These measures should include protecting detailed information on the type, category and quantity of the nuclear material, the schedule, route and timings of the shipment, physical protection arrangements, and the number, names and qualifications of personnel involved in the shipment. Particular consideration should be given to those operations involving Category I and II nuclear material.
- (19) The TSP will itself contain sensitive information on aspects of the shipment, including details of the packages and conveyances used to transport the material. Thus, the TSP should be handled in such a way as to protect the confidentiality of such information in accordance with the applicable provisions of the State. The entity responsible for preparing and submitting the TSP should follow the provisions determined by the State, taking all necessary precautions to prevent unauthorized access to any sensitive information contained in the TSP.

### **Trustworthiness of personnel**

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

## **SHIPMENT SECURITY**

- (21) Operating practices should identify equipment and resources that are to be used to reduce security risks. Such operating practices should be described in the TSP, including:
- (i) Choice and use of routes, where known, including identification of safe havens;
  - (ii) Use of guards;
  - (iii) Engineered systems to be used to enhance security;
  - (iv) Limiting access to nuclear material packages requiring the enhanced security level while in temporary storage en route.
- (22) This section of the TSP should include a general discussion of these practices, and specific subsections as follows.

### **Description of the nuclear material to be transported**

- (23) This section of the TSP should include information on the type of the nuclear material (i.e. plutonium, <sup>233</sup>U, <sup>235</sup>U or irradiated fuel), its category (i.e. Category I, II or III), the amount of nuclear material and its physical and chemical form, the isotopic composition and enrichment level, radiation levels and any other applicable data (e.g. age and burnup of irradiated fuels).

### **Description of the transport physical protection system**

- (24) This section of the TSP should describe the manner in which all of the elements that constitute the physical protection system for the transport of nuclear material are designed and maintained.

### **Packages and conveyances**

- (25) This section of the TSP should identify the packages to be used and any information on these designs that is pertinent to nuclear security. If specially designed conveyances are to be used, they should be described along with any protective capabilities those conveyances might provide (in terms of deterrence, detection and/or delay).

### **Planned and alternative routes and modes of transport**

- (26) This section of the TSP should contain a detailed description of the planned modes of transport and the planned primary routes to be followed, and all available information on these routes that would be useful to the State authorities, competent authorities, carrier personnel, guards and response forces.
- (27) This information should include, as applicable, current conditions that could affect the shipment: on relevant roads, railways and inland waterways; at port facilities, transfer and stopover facilities; at border crossings and airports. It includes:
- (i) Permissible speeds;
  - (ii) Areas where repair or construction work is being, or is expected to be, performed;

- (iii) Potential weather conditions;
  - (iv) Capabilities at planned transfer points and stopover facilities;
  - (v) Locations of refuelling sites;
  - (vi) Potential safe havens and subsistence locations.
- (28) Alternative routes that could be used in case of unforeseen circumstances should also be identified and described, including expected conditions on those routes and information similar to that reported for the proposed primary routes.

### **Physical protection measures**

- (29) This section of the TSP should describe how the shipper or carrier has designed its physical protection system to accomplish the objectives of deterrence, detection, assessment, delay and response. This section of the TSP should describe the physical protection measures that are proposed, recognizing that ensuring security during the transport of nuclear material is, in many ways, more challenging than at a nuclear facility. For example, it is difficult, if not impossible, to entirely preclude public access to shipments being made in public areas. Furthermore, an attempt at unauthorized removal, sabotage or other nuclear security related incident could occur anywhere along a transport route, which may extend over a significant distance and include remote areas, thereby giving an adversary a wide choice of potential attack locations. At some locations, it may be particularly difficult for adequate response forces to arrive within a useful period of time, in which case alternative response forces would need to follow the transport convoy at a reasonable distance.

### **Communications and positional tracking for normal operations**

- (30) This section of the TSP should describe the structure of the primary and alternative communications systems for the proposed transport operation. Any system proposed to be used for tracking the conveyances should be described. Such a system should be located at, and operated by, a transport control center or an alternative central point of communication if one is required by the competent authorities. Alternative communications systems, when required, should not be vulnerable to the same failure mode as the primary system in order to ensure at least one means of communication is available at all times.

### **Command and control for normal operations**

- (31) This section of the TSP should describe command and control procedures and designate the persons of authority for each phase of the transport operation. It should address the entire command and control arrangement for the shipment and define how it is coordinated with the communications structure and procedures. It should describe command and control procedures, designating the responsible authority and appropriate chain of command for each phase of the transport operation, making clear who has authority to make critical decisions for each phase, for routine situations or for response to an emergency or nuclear security event. When guards are used, the TSP should also define command and coordination procedures between the response forces and the

guards, and between the primary response forces and any secondary response forces that may be planned for deployment.

- (32) The chain of command should be described clearly and simply, and should define who has the authority to give the final decision to start, delay, cancel or interrupt the transport operation, and to take action in the event of an emergency or nuclear security event. It should specifically define the roles and responsibilities of the transport commander, the response force commander and the transport control center, and should specify how and when transfer of command and control would be made from the transport commander to the response force commander if this were to be necessary.

### **Maintenance and testing of systems and equipment**

- (33) This section of the TSP should address the manner in which all of the systems involved in the shipment are designed and maintained.
- (34) The section should also describe the inspection and testing of all equipment related to the shipment, to be performed prior to the beginning of the transport operations. Categories of equipment that should be inspected and tested before the commencement of a shipment include:
- (i) All transport conveyances;
  - (ii) Communications equipment and tracking systems;
  - (iii) Any delay systems (e.g. personnel barriers, vehicle immobilization systems) built into the transport packages or conveyances;
  - (iv) Weapons, tactical and protective equipment, and communication devices of guards and response forces.

### **Pre-shipment checks**

- (35) This section of the TSP should describe the competent authorities' requirements and the shipper's or carrier's arrangements for pre-shipment checks or readiness reviews.

## **RESPONSE PLANNING**

### **Emergency arrangements<sup>1</sup>**

- (36) This section of the TSP should address planned actions and procedures in the event of an emergency situation, such as a road closure, vehicle breakdown, vehicle accident or driver illness, that may occur during shipment. Emergency arrangements include, but are not limited to, availability of a backup vehicle and driver, capability for heavy towing and lifting, and plans for use of safe havens and alternative routes.
- (37) This section should also address the need and capability to immediately inform any transport control center or alternative central point of communication of any emergency

---

<sup>1</sup> This section refers to actions and procedures in the case of non-nuclear emergency situations and should not be confused with arrangements for response to a nuclear or radiological emergency.



situation, and for that control center or central point to be able to initiate the planned actions and/or procedures in response.

### **Contingency plans**

- (38) The TSP should designate specific individuals who have the responsibility and authority to carry out contingency plans if a nuclear security event occurs.
- (39) This section should also address the capability to ensure that any transport control center or alternative central point of communication can be made immediately aware of a nuclear security event and the time and place that it started. It should also address planned actions and procedures to be taken by the control center or alternative central point of communication should a nuclear security event occur.
- (40) The contingency plan should include procedures, such as the employment of guards and response forces, which will provide depth to the defences used during shipment. It should therefore identify:
  - (i) Any guards that are designated to accompany the shipment;
  - (ii) All response force units or organizations that are assigned responsibilities for the shipment;
  - (iii) Any other State assets that are projected to be available to support the shipment or assist in response to an incident or emergency;
  - (iv) All other support personnel, including fire, rescue and other services along the route, as applicable, and the communications system to be used to communicate with them.

### **Guards**

- (41) A graded approach should be used in deciding on the use of guards, and this should be reflected in the TSP. For example, the competent authorities may determine that the use of guards should be considered to accompany shipments of Category III nuclear material, whereas it should require guards to accompany shipments of Category I and II nuclear material. If armed guards are used, rules for the use of firearms should be clearly documented. If guards do not accompany the shipment, then the driver or operator of the conveyance, or another designated crew member, should be capable of providing surveillance of the nuclear material and of making any required notifications in the event of an attack or adverse conditions, in accordance with the information provided in the shipper's or carrier's TSP.

### **Response forces**

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

**Incident communications, command and control**

- (43) This section of the TSP should describe command and control procedures and arrangements, and communications structure and procedures, additional to those for normal operations, to be applied in an emergency situation.

### **APPENDIX III. VULNERABILITY ASSESSMENT**

- (1) For the performance-based approach and some variants of the combined approach, the administrative and technical requirements specified in the TSP should be evaluated against the prevailing threat or State DBT, using an appropriate vulnerability assessment.
- (2) If required by the State, the TSP should specify that the review of current or proposed transport operations and assessment of vulnerability will be conducted as appropriate, and that the resulting vulnerability assessment will be appropriately documented and used by the shipper, carrier or responsible authority in developing its physical protection measures.
- (3) The competent authorities may require that a vulnerability assessment be performed for the whole TSP or any part thereof that it considers warrants more detailed analysis, such as stopping points, route selection and transfer points. The vulnerability assessment may be a separate document classified appropriately and referenced in the TSP. The entity responsible for preparing and submitting the vulnerability assessment might not be the same entity responsible for preparing the TSP.
- (4) The assessment of the performance of any security system needs a methodical approach in which the ability of the system to meet stated requirements is determined.
- (5) The vulnerability assessment process comprises three major phases: planning the assessment, conducting it and concluding it.

#### **PLANNING THE VULNERABILITY ASSESSMENT**

- (6) A realistic evaluation of potential threats and their capabilities is an important aspect in undertaking a vulnerability assessment. In most cases, a vulnerability assessment will be a sufficiently complex process that explicit, detailed planning is needed to help to ensure that the assessment includes all necessary considerations, and that the objectives are met. The planning phase includes the following activities.

##### **Establishing the scope and objectives of the vulnerability assessment**

- (7) In the initial planning phase, it is necessary to determine the scope and objectives of the vulnerability assessment. Reference should also be made at this stage to relevant threat assessments and/or the DBT and to any constraints.
- (8) The scope of work should clearly define all expected deliverables and indicate the complexity and rigour with which the assessment should be conducted. The complexity and rigour of the assessment will depend on:
  - (i) The nature of the shipment, including the characteristics of the nuclear material;
  - (ii) The threat environment at the proposed time of shipment;
  - (iii) The time available to complete the assessment.
- (9) During transport, vulnerability may change dramatically at the different stages of the transport operation, for different modes of transport and for different routes.

### **Selecting knowledgeable team members, and defining roles and Responsibilities**

- (10) A team of experts may be created to ensure that a complete and accurate vulnerability assessment is produced. The team should include security specialists who can ensure that the vulnerability assessment is correct. The members of the team should collectively have knowledge of all of the main topics relevant to the vulnerability assessment, including physical protection systems, response actions, data analysis and managing radioactive contamination.

### **Developing a schedule with deliverables and resource requirements**

- (11) When developing the schedule, consideration should be given to setting a realistic time frame for the assessment and to any foreseeable risks that might prevent achievement of the objectives. All team members should be consulted to determine the resources needed to achieve the required results in the allotted time.

## **CONDUCTING THE VULNERABILITY ASSESSMENT**

- (12) The process steps within the second phase of a vulnerability assessment are:
- (i) To state the objectives of the physical protection system;
  - (ii) To describe the components of the physical protection system;
  - (iii) To characterize the components of the physical protection system;
  - (iv) To analyse the ability of the physical protection system to meet the objectives.

### **Stating the objectives of the physical protection system**

- (13) The vulnerability assessment starts with a statement of the objectives of the physical protection system for the shipment as provided by the competent authorities. This section may include relevant aspects of the DBT or threat assessment (if confidentiality considerations allow).

### **Describing the components of the physical protection system**

- (14) The tasks to be completed during this step of a vulnerability assessment include a description of the components of the physical protection system, the transport system, the nuclear material to be transported and, where applicable, the response forces.
- (15) A description of the transport system is important for establishing operational, safety and physical constraints on the physical protection system, as well as mode specific requirements. Understanding the material to be transported is important for applying a graded approach based on potential consequences of a malicious act and establishing performance requirements for the physical protection systems (preferably established by a separate consequence based risk analysis). The description of the response forces, if included, should include information on weapons, tactics and training.

- (16) This section should include applicable information on all phases of the proposed shipment, such as any planned intermodal transfer operations, temporary in-transit storage and sections of routes that pass through high and low population areas.

### **Characterizing the components of the physical protection system**

- (17) Characterization of a physical protection system involves gathering data, and often includes the development and validation of models, to determine how the human, procedural and technological elements of a physical protection system may be expected to perform against attack as postulated in the DBT or the threat assessment. In general, these elements are evaluated in terms of the ability to defeat an adversary, as effects of deterrence are difficult to quantify. Defeating an adversary may be broken down into the nuclear security functions of detection, assessment, delay and response. The measures used to characterize performance in respect of these security functions should support the input requirements for the analysis techniques to be used in the following performance determination step. Performance data are gathered by conducting tests at the component and element level.

### **Analysing the ability of the system to meet the objectives**

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

### **CLOSURE OF THE VULNERABILITY ASSESSMENT**

- (19) The last phase of a vulnerability assessment has the goal of providing an accurate record of the assessment. This should include descriptions of the methodology used, the assumptions made, the data collected and the results on the effectiveness of the physical protection system. The form in which the results are reported should be usable by those responsible for making decisions regarding the adequacy of the physical protection system evaluated. The reporting of results is typically conducted by two methods: briefings and written reports.
- (20) If the vulnerability assessment concludes that the physical protection system does not meet the established objectives, the documentation should include recommendations concerning potential solutions. Such solutions should be based on insights gained during the conduct of the vulnerability assessment and not on a detailed assessment of various design options. While the members of a vulnerability assessment team may be given responsibility for developing design recommendations in addition to conducting the vulnerability assessment itself, this should be considered a design upgrade activity and not an assessment of an existing physical protection system. On review of the results, the competent authorities and shippers or carriers may consider providing additional information to improve the scope or accuracy of the assessment in order to

address apparent disparities between security system requirements and performance projections. Because performance requirements are often based on risk assessments, changes in the material being transported (e.g. quantity) will alter the potential consequences of theft or sabotage, and thus may alter the conclusions of the assessment.

- (21) If the competent authorities consider that the State's requirements are not met by the vulnerability assessment or the assessment is otherwise inadequate, it should be returned to the originator for additional information and modification.

#### **APPENDIX IV. INTERNATIONAL TRANSPORT OF NUCLEAR MATERIAL**

1. Levels of physical protection for nuclear material during storage incidental to international nuclear transport include:
  - a. For Category III materials, storage within an area to which access is controlled;
  - b. For Category II materials, storage within an area under constant surveillance by guards or electronic devices, surrounded by a physical barrier with a limited number of points of entry under appropriate control or any area with an equivalent level of physical protection;
  - c. For Category I material, storage within a protected area as defined for Category II above, to which, in addition, access is restricted to persons whose trustworthiness has been determined, and which is under surveillance by guards who are in close communication with appropriate response forces. Specific measures taken in this context should have as their object the detection and prevention of any assault, unauthorized access or unauthorized removal of material.
  
2. Levels of physical protection for nuclear material during international transport include:
  - a. For Category II and III materials, transportation shall take place under special precautions including prior arrangements among sender, receiver, and carrier, and prior agreement between natural or legal persons subject to the jurisdiction and regulation of exporting and importing States, specifying time, place and procedures for transferring transport responsibility;
  - b. For Category I materials, transportation shall take place under special precautions identified above for transportation of Category II and III materials, and in addition, under constant surveillance by escorts and under conditions which assure close communication with appropriate response forces;
  - c. For natural uranium other than in the form of ore or ore-residue; transportation protection for quantities exceeding 500 kilograms uranium shall include advance notification of shipment specifying mode of transport, expected time of arrival and confirmation of receipt of shipment.