World Institute for Nuclear Security

A WINS International Best Practice Guide

GROUP 4: Implementing Security Measures

4.10 Nuclear Transport Security

Version 1.1

NUCLEAR TRANSPORT SECURITY

A WINS/WNTI International Best Practice Guide

Why You Should Read This Guide

The transport of nuclear and other radioactive material around the world is an essential activity to support the application of nuclear technologies for electricity generation, medical and other applications. Protecting these materials while they are in transit is an important consideration and one that requires cooperation between different organisations, each of which must have clearly defined accountabilities. The transport of material frequently involves organisations and agencies that are not generally responsible with the management of nuclear facilities, so excellent planning, coordination and communication are essential. So does an updated threat analysis covering publicly accessible locations such as roads and marine shipping routes.

For this reason, contingency plans need to be available and rehearsed in case the threat changes or materialises whilst the material is in transit. In many respects, the management of transport operations for high security nuclear cargoes can be more dynamic and challenging than the management of facility security, and special attention needs to be provided at all stages of the transport operation.

This guide has been produced to help identify best practices and the lessons learnt from the operational experience of transporting nuclear material classified by the IAEA as Category I and II (see IAEA NSS No. 13), and for transport arrangements involving road and maritime shipments. It is particularly important that the State, its nuclear regulators and the operators and carriers work together to ensure that the transport security arrangements are robust, and that the response to threats is effective and efficient. Transporters who are familiar with transporting Category III material will be able to use the guide as a review of what may be asked of them when considering the transport of Category I/II material.

About the Appendices

Appendices A and B provide a series of questions and levels of organisational competencies relating to transport security that will enable you to see how well your organisation is doing in this area and benchmark your performance. Results of this benchmarking process may indicate possible gaps in your transport security arrangements and could provide you with a starting point for improving the situation.

About the Preparation of this Guide

This guide has been prepared jointly by WINS and the World Nuclear Transport Institute (WNTI). In preparing this guide, we have taken note of the real-life experiences of organisations, including those that are transporting or protecting nuclear and other radioactive material in transport. This guide also reflects discussions from a Transport Security Table-Top Exercise (TTX) organised by the Government of Japan between the 12th and 14th November 2013 in Tokyo, Japan, as a preparatory activity for the NSS 2014. The guide also takes into account the draft IAEA Nuclear Security Implementing Guide titled *Security of Nuclear Material in Transport* (NST017) and is consistent with its guidance. Wherever possible, the guide uses the same terminology as that found in the IAEA Nuclear Security and Safety Series publications.

We Welcome Your Comments

We plan to update the information in this guide to reflect best practices and new ideas. Therefore, we ask that you read it carefully and let us know how to improve it. If you need help or assistance with any aspect of this guide, please email us. You can also contact us via the WINS or WNTI membership portal.

WINS Contact Information
World Institute for Nuclear Security Landstrasser Hauptstrasse 1/18 AT-1030 Vienna, Austria Email: info@wins.org Phone: +43 1 710 6519 www.wins.org

WNTI Contact Information
World Nuclear Transport Institute Aviation House 125 Kingsway London, WC2B 6NH, United Kingdom Email: wnti@wnti.co.uk Fax: +44 (0) 20 7580 5365 Phone: +44 (0) 20 7580 1144 www.wnti.co.uk

World Institute for Nuclear Security
Dr Roger Howsley
Executive Director

World Nuclear Transport Institute
Henry-Jacques Neau
Secretary General

March 2014

Version 1.1
ISBN: 978-3-903191-58-7
WINS(19)07

CONTENTS

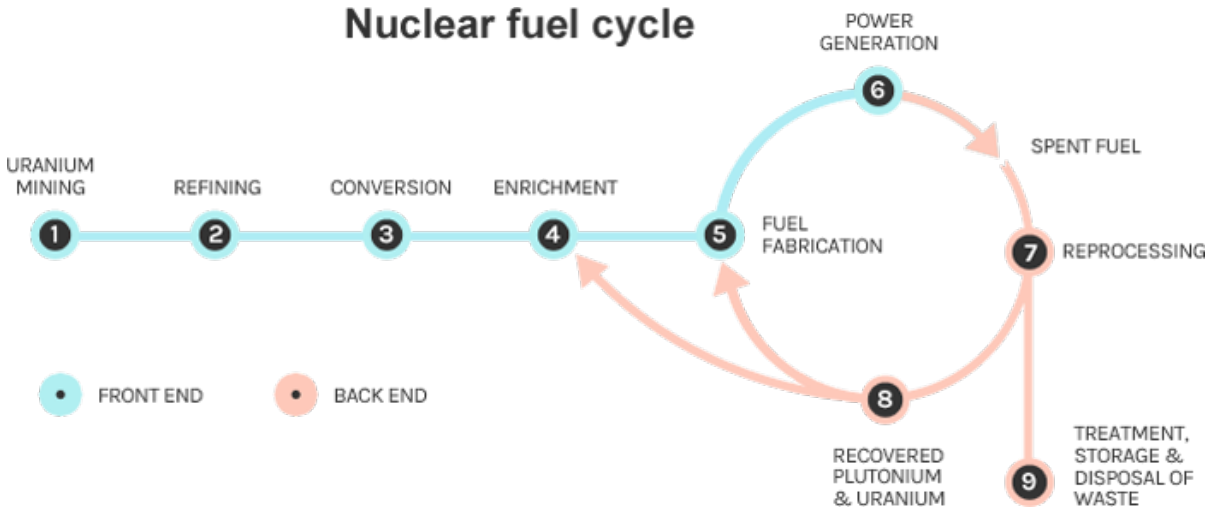
THE TRANSPORT OF NUCLEAR MATERIAL

A wide variety of nuclear and radioactive material has been transported safely for many years in order to support the generation of electricity, the application of radioactive material for medical and other purposes, and nuclear defence programmes (in some countries). About 20 million consignments of radioactive material take place around the world each year, the vast majority of which are of low radioactivity with very low associated risks.

Only few shipments contain material that needs higher protection for both safety and security reasons. In the civil sector, these are predominantly associated with shipments of separated plutonium and highly enriched uranium and with reactor fuels made from these materials.

Over 200 million packages of radioactive material are transported each year – most contain small quantities for medical, industrial or research purpose. Civilian nuclear power and some military activities give rise to a relatively small number of shipments with more significant amounts of nuclear material.

The following figure shows a simplified schematic of the closed civil nuclear fuel cycle, which is commonly described as having a front end and a back end. An open fuel cycle consists of shipping spent (or used) fuel directly from a power generation facility (item 6) to either storage or disposal facility (item 9).



The front end (items 1 through 5) typically consists of the stages from the mining of uranium ore up to and including the transportation of fresh uranium-based fuel to the nuclear reactors. Worldwide there are over 450 operating reactors producing 11-12% of the world's total electricity generation, each requiring periodic deliveries of fresh fuel. These shipments are typically classified as Category III or below based on IAEA guidance and are not the subject of this guide.

One exception is research reactors that produce radioactive isotopes for medical and other purposes and that may be fuelled with highly enriched uranium fuel (>20%). Another is power reactors that use mixed oxide (MOX) fuel, which contains plutonium. Shipments of these materials would be either Category I or II depending on the nature of the shipment and the amount of the fuel involved. They would need to be protected accordingly, both onsite and during transport. For transport operations, this would require special transport containers (also called flasks) carried by specialised road vehicles (high security vehicles or *HSV*s) and ships with accompanying escorts or guard forces.

The backend of the fuel cycle includes the operations concerned with the spent fuel discharged from the reactors. Such fuel either needs to be sent to reprocessing facilities for recycling (i.e. the closed fuel cycle) or sent to interim storage facilities pending final disposal (i.e. the open fuel cycle). Some of these facilities may be co-located with the reactors; in other cases, the spent fuel needs to be transported in the public domain.

Road Shipments

Reprocessing plants and MOX fuel fabrication plants are not necessarily on the same site, making transport between sites necessary. Road shipments of plutonium oxide are made in specialised transport containers and take place using HSVs. These are escorted by other security vehicles dedicated to protecting the shipment and to supporting the convoy, including maintaining communications among vehicles and with the control centre. Fabricated MOX fuel is also transported in specialised transport containers. Depending on their onsite storage capacity and other factors, reactors that use MOX fuel need 1-2 shipments a year on average to replace spent fuel assemblies. The distance that plutonium oxide or MOX is transported by road can be several hundred kilometres.

Maritime Shipments

For maritime shipments, there are generally two types of ships used for transporting Category I/II cargoes:

- Roll on/roll off vessels. These permit the HSVs to roll on and roll off the ship via a stern ramp. One advantage of these ships is that they allow the same HSV to travel the entire route without any need for the secure cargo to be transferred between vehicles. Transferring the cargoes is considered a point of potential vulnerability and is best avoided whenever possible.
- Other vessels, typically used for longer sea voyages, are constructed so that specially designed shipping flasks are loaded into the ship's hold and stored there under safe and secure conditions during the voyage. This method involves road/HSV shipments to the ports, the transfer of the heavy flasks into the hold of the ship, and offloading the flasks after port arrival. These ships are also subject to substantial physical security measures during the voyage.

CATEGORISATION OF NUCLEAR MATERIAL

The following categorisation table sets out the different levels of security requirements for the physical protection of nuclear material against unauthorised removal. Published by the IAEA, it ranges from Category I (highest security level) to Category III (lowest security level, other than un-categorised material).

Material	Form	Category		
		I	II	III[c/]
1. Plutonium[a/]	Unirradiated[b/]	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	Unirradiated[b/] ➢ uranium enriched to 20% ^{235}U or more ➢ uranium enriched to 10% 235U but less than 20% ➢ uranium enriched above natural, but less than 10% ^{235}U	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 10 kg but more than 1 kg 10 kg or more
3. Uranium-233	Unirradiated[b/]	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			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d/e/]	

IAEA Categories of Nuclear Material

[a/] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[b/] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 100 rads/hour at one metre unshielded.

[c/] Quantities not falling in Category III and natural uranium should be protected in accordance with prudent management practice.

[d/] 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.

[e/]Other fuel which by virtue of its original fissile material content is classified as Category I and II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 100 rads/hour at one metre unshielded.

DESIGNING AND IMPLEMENTING GOOD SECURITY DURING TRANSPORT (MANAGING THE RISK)

The following paragraphs describe the best practices identified by State authorities, regulators, operators, carriers and response forces. They have been grouped into the following sections:

International and National Framework

1. Developing an Adequate Regulatory Regime for Transport Security

INTERNATIONAL RECOMMENDATIONS AND GUIDANCE

The overarching convention relating to international transport (and in some respects, domestic transport) is the Convention on the Physical Protection of Nuclear Material (CPPNM). A subsidiary document, INFCIRC/225/Rev 5 (IAEA Nuclear Security Series No. 13) provides recommendations to States to establish, maintain and sustain an effective physical protection regime, including during transport. This guidance should be used by States as a basis for their domestic legislation and regulation. The Implementing Guides of the IAEA Nuclear Security Series provide further guidance for regulators, operators and carriers.

REGULATORY FRAMEWORK FOR TRANSPORT SECURITY

The establishment of a regulatory framework for security is the responsibility of individual States. Operators and persons engaged in the transport need to comply with these regulatory requirements, and there should be independent and effective oversight of the arrangements by a competent regulator. Frequently, however, it is the operator/carrier that has legal responsibility and liability for implementing the required regulatory arrangements. Consequently, it is important to have a clear distinction of responsibilities, including the organisation that has the 'controlling mind'.

> *It is essential that the Licensee retains the capability to be the controlling mind of those core activities for which the licence has been granted. Ceding that control to other parties would not be consistent with the principle that the licensee retains primary responsibility for [safety]' Nuclear Regulation, Nuclear Energy Agency, Report NEA/CNRA/R(2011)4.*

Security regulations should be developed taking into account the quantity and the physical chemical form of the material and the packages being used for the transport. It is also important to recognise there are synergies between the safety features of packages and security objectives.

It is good practice to involve all stakeholders, especially nuclear organisations and transport operators, during the development of regulatory requirements. Regular consultation between industry and the competent authorities can be beneficial in this respect. Some organisations have found it useful to exchange staff on secondment to broaden their experience and perspective.

Where possible, security regulations should be performance-based rather than based solely on prescriptive rules. This will give the operator more flexibility in developing the security requirements and ensure that accountability for effective security implementation rests with the operator/carrier.

2. National and International Considerations

When the consignor and consignee are under the same jurisdiction and legislation (i.e. within the same State), transport of nuclear material is generally less complicated than for international transport. By comparison, international transport may involve different States that need to be co-ordinated because of the change in jurisdiction and possible stopovers and changes of mode of transport.

Where there is a cross-border transfer of responsibilities, responsibilities for the security arrangements must be discussed and agreed in advance between the two national competent authorities. Specific attention should be given to language and cultural differences to avoid misunderstandings. For international shipments, agreement should be reached in advance on the different aspects of the security arrangements that are relevant to the transport, including such matters as:

- The sharing of threat and risk information to enable the route to be planned and agreed.
- Responsibility for updating the threat assessments during the remainder of the transport.
- Assurances relating to the trustworthiness of personnel involved with the shipment.
- Arrangements for the maintenance of tracking information to maintain knowledge of the shipment location, where agreed.
- Provision of secure locations for any scheduled or unscheduled breaks.
- The handover arrangements for armed personnel and other escorts, including safety and medical support.

Inter-governmental agreements may need to be concluded well ahead of time particularly where armed guards are employed.

3. Identifying Roles and Responsibilities

Although the competent authorities are responsible for approving the security requirements, operators, consignors and consignees should strive to engage themselves in all aspects of the preparation. Because the transport organisations are specialists, it is likely that they are aware of best practices in other sectors that require high security arrangements and can propose improved methods of working based on this broader experience.

Regulators and practitioners both emphasise that the development of transport security plans (TSPs) requires the personal engagement of all parties to help ensure that the documented TSPs are genuinely effective, with clear and unambiguous accountabilities and duties. This necessitates a programme of meetings and discussions, including tabletop exercises and other scenario-based exercises, to test the resilience of the planning, the adequacy of the security arrangements, and the assumptions made about roles and responsibilities. Resilience and empowerment to take decisions are essential features of the transport planning arrangements, as are an effective chain of command and communication.

CARRIER RESPONSIBILITIES

Carriers have the responsibility to comply with the regulatory requirements defined by the States and any other provision detailed in the TSP or applicable requirement document. Prior to commencing transport, the carrier should verify that all physical protection measures are in place. Carriers must ensure that the nuclear material is always under continuous supervision and control and that any transfer to another carrier or to the receiving organisation is clearly defined. The carrier should inform the consignee of any changes to the agreed plan, including any changes to the expected time of arrival. The carrier should also be fully aware of its liability for the shipments, including aspects relating to insurance, and the costs and responsibility of any escorts.

Competencies and Planning

4. Managing Individuals Engaged in Transport Operations

COMPETENCY BASED TRAINING AND CERTIFICATION

The consignor/carrier/consignee and competent authority should ensure that all personnel involved in the transport arrangements and security are suitably trained and qualified, commensurate with their roles and responsibilities. Training should be designed and provided to a high standard, be directly relevant to the TSP, and ensure that personnel are demonstrably competent. In some States and for some positions (such as a Ship's Security Officer), there are regulatory requirements for relevant staff to be certified to hold positions of security and managerial accountability. (This is considered best practice.)

It should be remembered that in the event of an incident and subsequent inquiry, investigators are likely to require evidence relating to training records (this is commonplace after aviation incidents). Consequently, it is essential that all personnel be demonstrably competent. It also makes good sense operationally. Where there is a high turnover of staff positions, staff will not have time to receive on-the-job training, so they need to be given structured trainingbefore taking up their responsibilities.

PERSONNEL RELIABILITY

Implementing effective TSPs relies on both the reliability of the transport and security systems and on the personnel associated with the transport. All personnel involved with high security transportation should undergo background security checks (reliability assessments) commensurate with their responsibilities and access to sensitive or classified information and material. Such checks need to be completed in advance of transport operations and should be reviewed periodically.

The nature of transport operations means that there may be many different personnel that have some ancillary involvement with the operation, including port workers, maintenance engineers, catering suppliers, etc. If it is impractical to require all such personnel to undergo reliability checks, then best practice is to undertake a risk assessment to ensure that their actions cannot significantly interfere with or degrade the security arrangements. This may require personnel supervision, security inspections and checks before departure as well as measures to ensure continuity of knowledge concerning the integrity of the consignment.

CONTINUITY OF PERSONNEL

Personnel responsible for high security transportation need to have the required training and adequate experience to undertake their duties. It is also important that they form strong and reliable teams where trust and respect are generated through working partnerships. Practitioners highlight the importance of continuity of employment and the time it takes to build teams in which there is high confidence. For this reason, changes to the teams need to be managed with care and new personnel should be subject to induction programmes. Sharing experience and best practices both at a national and international level is important to building competence and capabilities. Personnel from experienced organisations have expressed their willingness to provide advice and coaching to less experienced organisations, where necessary.

5. Security by Design

Transport containers used for the shipment of spent fuel, high-level radioactive waste and MOX are typically known as 'Type B' packages. Such containers must pass performance standards defined by the IAEA in the Regulations for the Safe Transport of Radioactive Material (SSR-6). The standards relate to the integrity of the container under adverse conditions. In addition to demonstrating the safety characteristics, the testing results may also be relevant to the security arrangements. For example, the integrity of the container and its inherent resistance to stress testing is one of the design features that may be considered when assessing the overall security of the consignment. Other design features, often of a classified nature, are associated with consignments and need to be able to withstand the assessed scale of attack for a sufficient duration. In common with nuclear facility security, there are advantages to designing security into the transport vehicles and associated equipment to enhance their resilience.

6. Use of Modelling and Simulation for Transport Security

Modelling and simulation techniques are being increasingly used as a planning tool to evaluate the security requirements for nuclear facilities, but they have not been widely used for transport operations. This may change as the modelling and simulation systems become more advanced. Some operators have found standard techniques, such as fault tree analysis, useful for analysing possible fault conditions caused by both safety and security events. Certainly, adopting an all-hazards approach to risk analysis is considered best practice.

7. Safety and Security Interfaces

Inevitably there is an interface between the safety and security features of transport equipment and operations. Some of these features are perceived as advantageous whilst others can cause potential difficulties. For example, the robustness of the package provides a certain degree of security; the physical weight of the package means it cannot be easily transferred from one transport vehicle to another without special lifting appliances. In this sense, the safety features support the security objectives.

However, there are also potential conflicts between safety and security objectives. Some States (and relevant regulators) require that all nuclear transport operations be clearly identified by attaching safety placards and incident labels to the conveyance. This is intended to help emergency responders understand the nature and characteristics of the cargo. However, other States believe that labelling conveyances in this way attracts undesirable attention to the shipment and is unnecessary since the shipments are accompanied by knowledgeable escorts and equipped with communication systems in the event of an incident.

The speed with which the transport operation travels is also a point of potential conflict. For security reasons, the time should be minimised and wherever possible the operation should be continuous and not involve unnecessary stops or delays. From the viewpoint of safety, the opposite is often preferred, with slow speeds and frequent interruptions to rest the transport crews and check safety systems.

One of the most important aspects of planning is to decide in advance whether a malfunction of equipment associated with the operation is likely to have been caused by the inadvertent failure of the equipment (which could have safety implications) or whether all such events are presumed to have potential implications for the security of the transport. For example, if a road vehicle experiences a tyre failure, is the immediate assumption that this is a safety issue or that the tyre could have been intentionally damaged as the start of an attack?

This assessment and the subsequent decisions that are made will have an important influence on the planning and response arrangements. Some States presume that incidents such as this must be considered from a security perspective and that the security of the transport, especially for Category I/II cargoes, is of paramount importance. Such issues need to be considered by the relevant parties during the planning phase, and agreement needs to be reached on the optimal arrangements.

8. Developing a Transport Security Plan

IMPLEMENTING A GRADED APPROACH: VULNERABILITY ASSESSMENT

Clearly, the type of nuclear material, as well as its form and quantity, will contribute to the security requirements for the transport operation. The Convention on the Physical Protection of Nuclear Material (CPPNM) defines the basis on which nuclear material is categorised. In each case, the regulator and the operators need to consider the potential forms of attack and whether the material being transported is principally at risk from theft or sabotage, or both, and whether the potential consequences of a successful attack are principally concerned with radiological contamination or with the theft of material that could be used for malicious purposes. The vulnerability assessment helps inform the security arrangements because it allows scenarios to be developed that attempt to predict the methods that could be used by attackers and to help ensure that the security systems are effective against the postulated threats.

THREAT ASSESSMENT

The State is responsible for obtaining, collating, analysing and disseminating threat information to relevant organisations involved in the transport of nuclear material, as well as for ensuring that the information is thorough and current. The detailed threat assessment and analysis are likely to be sensitive and classified, but the State should make relevant, summarised information available to those with security responsibilities for the transport operation (with suitable precautions and controls over its communication). It is likely that the State will define a baseline threat assessment that can be used for planning purposes, but this should be reviewed and updated before the Transport Security Plan is approved.

The accountabilities for threat assessment should be clearly defined in the planning documentation since this forms an essential component of the risk assessment associated with the transport operations. Operators often have specialised knowledge of transport routes and potential problem areas that should be avoided when planning the route or other transport arrangements. Consequently, they should be encouraged to contribute to the assessment process. International shipments may require threat assessments to be performed by more than one State or a mechanism to share threat assessments that relate to the transport route. Agreements will need to be reached between States on how this is best achieved so that there is confidence in the planning process.

9. Exercises

All personnel with accountabilities for transport operations and security should be required to demonstrate a full understanding of their roles and responsibilities before the transport takes place. Exercises can take a variety of forms; best practices for such exercises are reviewed in the WINS International Best Practice Guide on Security Exercises (see Further Reading). It is essential that the exercises be as realistic as possible and challenging. The scenarios must establish the resilience of the plans, and the exercises must involve the different agencies and personnel that have accountabilities.

Experience has also shown that exercises should be performed in a constructive way, with the objective of identifying areas for improvement. They should not be used to apportion blame or criticise individuals. Participants in the exercise also need to have the confidence to propose areas for improvement. The outcomes of the exercise should be to validate and test the security plans/procedures, provide a learning environment, and develop staff competencies and teamwork.

Some organisations make use of independent experts who specialise in emergency planning and crisis management to help ensure that the exercises are managed effectively and from an experienced and independent perspective. This also helps to keep difficult issues from being ignored or overlooked. Experience has shown how important it is to avoid false confidence in the arrangements, especially by those who have written the plans. Performance measures are also important to give focus to the transport operation and to ensure that the security arrangements are able to respond effectively to the various scenarios.

10. Preparing for the Transport

PLANNING APPROVALS AND IMPLEMENTATION

Once the transport arrangements have been approved by the relevant authorities, the agreed physical protection measures adopted in the plan must be adhered to. If there are any reasons that the physical protection measures cannot be implemented in accordance with the plan, the carrier should implement mitigation measures and inform the relevant authorities as soon as possible.

Carriers should ensure that the TSP bears an appropriate protective marking and that it remains protected in accordance with national requirements. In the case of international shipments, it may be necessary for the TSP, or parts of it, to be shared with foreign organisations. Where no national protocols exist in this area, carriers should ensure that contractual conditions are specified to guarantee the continued protection of sensitive information.

ROUTE SELECTION

Land Transport

For road transports, there may be differing routes available to a consignor between the start and destination points of the consignment. Each route has to be evaluated and assessed for its appropriateness. Routes should not only be appropriate for the vehicles used, but also for the escort vehicles, taking into consideration the overall constraints of the vehicles and escort procedures. The journey time also has to be considered; the shortest route may not be the most secure as it may transit through areas of potential unrest or natural faults. The response time to an incident on a particular route should also be considered.

Maritime Transport

For international maritime transport, the route selection is less constrained than for land transport, especially when in non-coastal open waters. In open waters, a vessel can observe other vessels, manoeuvre and take avoiding action, and generally be more aware of whether other vessels are behaving in a way that indicates they may be a threat. Response times to an incident that occurs in the deep sea may be considerable. This needs to be factored into the security arrangements for the cargo so that adequate protection and delay are provided.

For maritime transport in coastal waters, a vessel is more restricted by navigational constraints such as draft, water depth, navigational marks, navigation separation zones, land, islands and other shipping. There is likely to be more shipping traffic in coastal waters, especially close inshore which could hide potential threats. However, shore-based electronic navigational tracking systems are available to ensure the safety of navigation and may be used to assess potential threats.

LAND TRANSPORT STOPOVERS

Planned stopovers

Whenever possible, stopovers should be avoided. Unavoidable stopovers because of long journey times (and in some cases, the time involved with crossing international borders and clearing customs) need to be planned well in advance so security requirements are not compromised during the layover. Any exchange of responsibility during the stopover must be clearly defined. For Category I/II cargoes, it is preferable to identify secure locations for any stopovers, including government controlled locations and other nuclear facilities, that already have significant security arrangements and personnel with relevant experience and security clearances. The controller of command and control centres must be kept informed of arrival and departure at planned stopovers.

Unplanned stops

There may be unplanned occasions when a convoy will be forced to stop. An example would be a mechanical fault with a vehicle in the convoy. The command and control centre must be immediately informed of any non-planned stop, and the communication lines should be kept open and clear during the stopover. All personnel associated with the transport should be put on a high level of alert in accordance with procedures that have been defined in the TSP and exercised.

INTER-MODAL TRANSFERS

Category I/II transports often involve inter-modal transfers at ports or rail heads. Consequently, the security plan should cover the measures/procedures that must take place when material is transferred. Such locations are often in the public domain, and arrangements may need to be coordinated with multiple agencies with different responsibilities and priorities. Access to the transfer area should be limited to the minimum number of personnel necessary to conduct the transfer safely and securely. Arrangements for dealing with protest action should be considered in advance as part of the TSP and coordinated with relevant law enforcement agencies. Confrontation between protestors and any guards accompanying the shipment, especially when armed, should be avoided as far as possible.

PRE-SHIPMENT CHECKS

Pre-shipment checks (Readiness Reviews) are important for ensuring that all measures described in the security plan are in place and functioning and should therefore form part of the quality management arrangements. Checks should include all administrative, personnel and equipment components and should identify any deficiencies and required corrective actions. If it is impossible to correct any identified deficiency prior to a planned transport, carriers should take advice from their competent authorities as to whether the transport can take place or if it needs rescheduling.

11. Information Security

When developing their regulatory framework for information security, States should identify and define which transport information is sensitive and needs to be protected. This information should not only address routes, times and the quantities of material but also escort forces, response forces, back-up personnel, design and security measures of the package, and the conveyance. Several different State agencies may be involved in the transport operation, each with their own rules for information protection. If so, procedures may have to be established for information exchange and sharing.

Good practice for information security includes:

- Avoiding *blanket classifications*. All documents/information related to transport operations should be classified the same, irrespective of sensitivity.
- When preparing documents, it is important to consider whether sensitive details can be omitted so the documents do not need to be classified. A good practice is to imagine that the information becomes compromised. What would you wish you hadn't included in the document that wasn't absolutely necessary? This is particularly the case with information held electronically that can be intentionally or inadvertently forwarded to other persons that may not be authorised to receive the information.
- Be aware that the sensitivity of information and the classification it attracts can change with time—sometimes very quickly. For example, information about sensitive transport operations may be confidential before or during the operation but can be released afterwards. Transport operations usually use public routes (rail, road, air, etc.), and there may be people that take an interest in and monitor transport operations. If this is the case, operators can lose credibility if they either deny the transport operation is occurring or maintain that all details are confidential.

- Most nuclear transports require a large number of people to be aware that a transport operation is going to happen, many of whom have no specific involvement with the details or security of the shipment. Examples inlcude ancillary workers who provide services such as catering or safety-related services and who become aware that a shipment is planned. Good advice is to adjust the information security plan accordingly, because applying classified rules when the information is widely known undermines credibility.
- It is also important to recognise and prepare for the fact that information, which may be classified at a particular level during normal operations, may need to be shared with unauthorised persons in the event of an emergency. Examples include staff, contractors, emergency responders, and the media. Consequently, plans need to be in place to manage the response effectively.
- Information relating to the physical protection arrangements of a convoy should be protected after the shipment to the extent possible, especially if the same arrangements are to be used again. (Additional information is available in the WINS International Best Practice Guide entitled Information Security for Operators: Challenges and Opportunities.)

Because information security can be challenging for international shipments, an agreement on what is to be kept confidential should be reached between the independent States at an early stage.

Transport Operations

12. Monitoring and Tracking Shipments

There has been a rapid advance in communication systems over recent years, which means there are now many different ways to communicate with and track transport operations. Tracking of international shipments of differing commodities is now offered as a standard practice by many road/truck and maritime companies, and all Category I/II shipments should be tracked using secured communications.

An electronic tracking system can provide instant and automatic alert/alarm notification to support incident response and emergency management arrangements and to monitor such parameters as radiation levels and the correct functioning of devices. The best systems are characterised by excellent encryption, very high reliability, few false alarms, ease of use and reasonable cost. One of the most important benefits of electronic tracking systems is that their automatic alarm notification capabilities decrease response times in the event of emergency. Because monitors know where the alert is coming from, they can provide emergency services with the exact location of the shipment—whether it is static or in motion—far faster than is possible with any other means.

A second benefit is that such systems can be highly efficient and cost-effective. Because tracking and monitoring are done automatically and continuously, personnel can determine, with reasonable certainty, when a load will pass through certain checkpoints and when it will arrive at its destination. This enables support teams to be deployed at the right time. A third benefit is that electronic tracking systems create a fully-logged history of every step the cargo has taken. This helps to reassure operators that no interference has occurred.

Electronic tracking can detect unplanned door openings, emergency stops, the unhooking of a trailer, and movement of or interference with packages. Such capabilities provide added confidence and assurance. (Further information on electronic tracking for the transport of nuclear and other radioactive material is published in the WINS/WNTI International Best Practice Guide - Electronic Tracking for the Transport of Nuclear and other Radioactive Material.)

Responsibility for monitoring the transport operation may belong to the carrier, the escort commander, or both. Some national regulators specify how these arrangements are to be implemented. The important criteria relate to the reliability of the systems (best practice is to have independent, redundant systems), as well as the degree to which a rapid response can occur should an incident occur. The role of a centre for monitoring and communication is extremely important and supports command and control decisions. It should be able to monitor and assess the situation as the transport progresses and to advise the escort/guard forces of any change in the threat or circumstances that may affect the transport. The centre should also have the capabilities, authority and ability to understand the terms of engagement and to call on additional forces if required.

13. Command and Control

The term *Command and Contro*l may mean different things to different communities, so it is important to understand that there are different approaches to accomplishing the functions of a command and control operation. All entities involved during a transport operation, including operators and safety/security personnel at the scene and in monitoring/control centres, must understand the distinctions between command and control during normal transport operations and the arrangements that will be put in place during an incident.

These arrangements need to be fully tested and understood during training exercises so that there can be no doubt as to what they are in the lead-up to an incident, during the incident itself, and during the recovery phase. In particular the armed response force will need to be aware of the command and control arrangements:

- In the proactive phase in response to intelligence of a terrorist or criminal threat,
- During the period of crisis as an incident or emergency occurs,
- During the recovery phase from an incident.

For the armed escort team, a particular issue on which there needs to be complete clarity is the situation as regards command of their actions. Do they fall under the command of the operations transport manager? In the case of a maritime shipment, do they fall under the Ship's Master? Do they have the power to take whatever actions they deem necessary? If additional forces arrive to reinforce the convoy, do the armed personnel become subject to the command of the incoming force? Answers to such questions will vary from jurisdiction to jurisdiction. Whatever the arrangements, they need to be fully understood and tested in exercises.

Key to all of the above will be reaching a shared understanding between all parties as to the underlying philosophy that governs command and control during all phases of the transport operation. In some jurisdictions, the rule will be that one person is in overall command of all elements of an operation, with subsidiary functional command chains below him/her. In other jurisdictions, there will be a different approach.

In a modern, interconnected world, with many interdependencies and complexities, it is generally not feasible for one person to exercise personal command of the entirety of a complex operation. Instead, the person in charge becomes in effect a co-ordinator and exercises effective command through agreement of the participating parties. This approach can be extremely effective, but it requires that all parties agree beforehand to the arrangement, recognise the need to agree, and have previously worked and exercised together.

Response to Incidents and Crisis Management

14. Contingency Plans

Contingency plans should be developed for all anticipated scenarios and for as many situations as possible. The contingency plans should be built into exercises and training programmes and should be rehearsed and reviewed as many times as required. Within the contingency plans, there should be performance indicators to assess if the required outcome is being achieved.

ESCORTING THE TRANSPORT

Escort requirements

The escort configuration will depend on the nature of the shipment. Aspects that may be considered when assessing the configuration of the escort team include the duration of the transport, the sensitivity and attractiveness of the material, the remoteness of the transport, the time required to deploy extra forces, the reliability of communication systems, the number of packages within the conveyance, and the number of conveyances within a convoy.

There are private organisations that offer armed escort and protection measures, including for maritime shipments (largely in response to the high incidence of maritime piracy in recent years). since their introduction for merchant vessels, no ship with armed protection has been successfully attacked by pirates. Use of such organisations depends on the jurisdiction that applies; the transport route may not be not supported or approved by all countries.

Consideration should also be given to whether the transport team includes medical support, whether this is a dedicated paramedic support team or whether the escort guards are trained in paramedic skills and whether appropriate medical supplies are carried by these individuals.

Co-ordination between escort and response forces

There must be a clear definition of command and control between an escort force and any independent response force that may be called on to provide reinforcement and support. Because it must be clear where the responsibilities change from one force to the other, there must be a well-established chain of communication between the two command structures. The change of responsibilities must be exercised so that it is seamless and fully understood who is in command of the situation at a particular time should an event occur. The communication systems and any firearms the two forces may carry also need to be compatible.

Rules of engagement

Domestic law is clearly the predominant factor in determining Rules of Engagement and the appropriate use of force. Nevertheless, international standards should also be considered when considering the thresholds at which the use of deadly force might be justified. A recurring theme is whether the particular risks associated with the potential harm that could be caused by a malicious release or theft of nuclear material could justify different Rules of Engagement from those that would apply in non-nuclear environments.

For instance, would an unauthorised approach to a high security transport operation ever justify the use of deadly force in the absence of some overt indication of an intention to attack the convoy? In what circumstances would a failure to obey directions from a guard force member justify the use of firearms? It is possible to conjure up numerous scenarios where these and other questions can be asked, and each transport operator and response force will have particular concerns that could prompt similar questions. For the trainer of the armed guard force, the real question is whether the training being given is both tactically and legally sound.

It could be a mistake to assume that the particular hazards associated with the nuclear environment will in themselves justify a different approach to the use of force to that which is generally permitted within a particular jurisdiction. Legal advice needs to be taken and exposed to a range of testing scenarios. Only in this way can both trainers and officers be sure that their training and tactics are legal and will not give rise to personal or corporate liabilities if an incident should occur.

As well as considering the use of lethal force, the training of the escort guard force needs to encompass the use of less-than-lethal options. This is particularly relevant when it comes to examining the tactics that are applicable to dealing with unarmed protesters. In some jurisdictions armed officers must not be used for public order duties or where they are likely to come into close physical contact with an unarmed opponent. As with the use of firearms, each jurisdiction will have a legal and doctrinal position on this subject, but it also needs to be considered specifically in the context of the nuclear industry. The subject is explicitly addressed in the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, General Provision 2.

> *Governments and law enforcement agencies should develop a range of means as broad as possible and equip law enforcement officials with various types of weapons and ammunition that would allow for a differentiated use of force and firearms. These should include the development of non-lethal incapacitating weapons for use in appropriate situations, with a view to increasingly restraining the application of means capable of causing death or injury to persons. For the same purpose, it should also be possible for law enforcement officials to be equipped with self-defensive equipment such as shields, helmets, bullet-proof vests and bullet-proof means of transportation, in order to decrease the need to use weapons of any kind.*

General Provision 4 of the same document takes this further:

> *Law enforcement officials, in carrying out their duty, shall, as far as possible, apply non-violent means before resorting to the use of force and firearms. They may use force and firearms only if other means remain ineffective or without any promise of achieving the intended result.*

Best practice is to ensure that there is sound legal advice before any shipment involving armed guards takes place and that the training and tactical planning is in accordance with that advice.

Gaps and overlaps

It is important to avoid gaps and overlaps in accountability during the handover of responsibilities. Particular attention needs to be given at this time to regional or national boundaries, different organisations, such as a reinforcement team, and in areas such as harbours where the coast guard, land-based police and security personnel reporting to the harbour master may each have their own responsibilities. The most effective way of resolving these potential issues is to ensure that dialogue takes place between the various parties and leads to written agreements on accountability and to the deployment of joint exercises that test the arrangements in practical and realistic settings. (Avoiding overlaps in responsibility is just as important as avoiding gaps in responsibility.)

15. Media Communications Following an Incident

Any security incident during a transport operation is likely to attract national and international media attention. The government, operator and their senior managers will generally have the responsibility to deal with media enquiries, so there needs to be an agreed strategy in place along with identified spokespersons. If an incident occurs that involves the deployment or use of firearms, it is inevitable that there will be a sharp focus on that aspect of the incident. It is therefore important that the security manager or armed force commander be aware of the overall media strategy and have the ability to contribute in a timely and effective way on firearms issues. Questions to answer include:

- What is the media strategy? Who has formulated it? Who has approved it? Who has the lead responsibility for co-ordination and delivery of it during and after a crisis?
- Has the armed force been consulted on those aspects that are relevant to them?
- What are the mechanisms for ensuring that references to the armed force and their work do not risk compromising the current operation? There are many instances where media coverage has jeopardised lives and operational outcomes through live broadcasts of operational activity. What are the arrangements for negotiating with media organisations to prevent this happening?
- What are the arrangements for collaboration with other agencies to ensure that the media strategy is fully co-ordinated and does not have any adverse operational impacts?
- How will the fact that the convoy was carrying nuclear material influence the media strategy? A likely issue is the constant demand from the media for reassurance public safety was not compromised. In the context of a nuclear transport operation, who could or should be in a position to offer such reassurance?
- Should a representative of the armed response force need to give a statement or interview to the media, is there someone at an appropriate level who is suitably trained and qualified to fill the role?

Experience has shown that there are benefits to investing time with the media before major transport operations take place. They should be given unclassified, but relevant, information and the opportunity to ask questions that do not compromise security. News travels fast, and bad news travels faster, so the communications strategy must be effective and timely. Messages need to be concise, truthful and consistent to the extent possible in an evolving situation.

Review and Learning from Experience

16. Assessing the Effectiveness of the Security Measures a nd Continuous Improvement

KEY PERFORMANCE INDICATORS

Key performance indicators (KPIs) should be set within the TSP and support a continuous assessment and improvement process. The plan should indicate the quantitative and qualitative evaluation processes that will allow for a timely identification of issues and recommendations for improved performance standards. Such KPIs can be evaluated during actual transport operations or exercises of the transport plan. It is crucial that a spirit of continuous improvement exist within the organisations and that they constantly seek more effective and efficient ways to improve the transport operations.

LEARNING FROM OTHERS

There are lessons to be learnt from previous transports and operational experience. There are also many other industries that protect their materials whilst in transport, such as bullion and cash shipments and the diamond industry. Lessons can be learnt on how such industries survey their routes and how they provide emergency response in case of an incident. Both the nuclear industry and State entities are encouraged to interact and learn from other industries and share past experiences of shipments of Category I/II material with each other. It is especially important to help States and operators who are planning to ship such cargoes for the first time. This sharing of experience and best practices can be achieved through workshops, tabletop exercises, best practice guides, coordination through nuclear-related organisations such as the IAEA.

FURTHER READING

IAEA. (2012). *Communication with the public in a nuclear or radiological emergency*.

IAEA. (2012). *Communication with the public in a nuclear or radiological emergency – Training materials.*

IAEA. (2013). Joint Radiation Emergency Management Plan of the International Organizations EPR-JPLAN.

IAEA Nuclear Security Series Publications.

NSS No. 8 (2013). *Preventive and protective measures against insider threats*.

NSS No. 9 (2008). *Security in the transport of radioactive material.*

NSS No. 13 (2008). *Nuclear security recommendations on physical protection of nuclear material and nuclear facilities* (INFCIRC/225/Revision 5).

NSS. No. 20 (2013): *Objective and essential elements of a state's nuclear security regime*.

IAEA. (2012). *Operations manual for incident and emergency communication.*

Industry guidelines for the security of the transport of dangerous goods by road. (2016). Retrieved from http://www.cefic.org/Documents/IndustrySupport/RC%20tools%20for%20SMEs/Document%20Tool%20Box/Security%20Guidelines%20of%20the%20transport%20of%20dangerous%20goods.pdf

International Road Transport Union. (2005). *Road transport security guidelines—Voluntary security guidelines for managers, drivers, shippers, operators carrying dangerous goods and customer-related guidelines.* Retrieved from https://www.iru.org/sites/default/files/2016-01/en-security-guide-goods.pdf

United Nations. (1990). Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, General Provision 2. Retrieved from http://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

WINS International Best Practice Guides. Available to members at www.wins.org.

4.8 *Electronic Tracking for the Transport of Nuclear and other Radioactive Materials*
4.6 Security Exercises
2.3 Information Security for Operators: Challenges and Opportunities

APPENDIX A

QUESTIONS TO ASSESS THE EFFECTIVENESS OF THE SECURITY ARRANGEMENTS FOR THE TRANSPORT OF NUCLEAR MATERIAL

The questions in Appendix A will help you evaluate the effectiveness of the security arrangements implemented for protecting nuclear material during transport. Using the questions as prompts for generating discussion will help individuals in various organisation reflect critically on their actions and behaviour and identify how they can contribute personally to developing, implementing and enhancing an effective security programme for transport operations.

Questions for the Nuclear Operators (Consignor)	
Do you believe a credible threat (theft or malicious act) exists to your nuclear material while it is in transit?	☐ Yes ☐ No
Would the reputation of your organisation be damaged should there be an incident during transport?	☐ Yes ☐ No
Do you understand your potential liabilities in case of an incident?	☐ Yes ☐ No
Have you established clear responsibilities and accountabilities for transport security?	☐ Yes ☐ No
Have you been involved in the design of the transport security plan?	☐ Yes ☐ No
Do you receive necessary information on possible threats to your materials while in transit?	☐ Yes ☐ No
Do you receive information on the location of your materials while in transit?	☐ Yes ☐ No
Does your contract with the carrier cover security arrangements?	☐ Yes ☐ No
Are you satisfied with the level of skills and competences your staff possesses in transport security?	☐ Yes ☐ No
Are you involved in the control and command structure in case of incident?	☐ Yes ☐ No
Do you have a media communication plan to be activated in case of security incident?	☐ Yes ☐ No

Questions for Transport Operators (Carriers)	
Do you understand your potential liability in case of security incident?	☐ Yes ☐ No
Do you receive sufficient information on possible threats that could affect your shipments?	☐ Yes ☐ No
Do you thoroughly understand the requirements for transport security imposed by the States from, through and into which your shipments will travel?	☐ Yes ☐ No
Does the transport security plan clearly define roles and responsibilities of organisations and individuals involved in transport security operations?	☐ Yes ☐ No
Have you performed a vulnerability assessment of the transport security arrangements?	☐ Yes ☐ No
Do you periodically exercise the transport security arrangements?	☐ Yes ☐ No
Do you have arrangements in place to benefit from operational experience, lessons learned and good practices from other carriers, the nuclear industry and other sensitive industries?	☐ Yes ☐ No
Do you promote the concept of a 'spirit of continuous improvement'?	☐ Yes ☐ No
Do you perform readiness reviews on the operation of your security systems prior to every shipment?	☐ Yes ☐ No
Have you identified a list of possible malfunctions or failures of security equipment and their impact to security?	☐ Yes ☐ No
Can you permanently track and monitor your shipments?	☐ Yes ☐ No
If the security system detects a possible threat to the integrity of a package or transporting conveyance, will an alarm immediately notify a continuously staffed control centre?	☐ Yes ☐ No
Are all personnel involved with shipments suitably trained and qualified commensurate with their accountabilities for security? Can you demonstrate their competence?	☐ Yes ☐ No
Do you have an insider mitigation programme? Do you have specific measures to ensure staff reliability?	☐ Yes ☐ No
Do you have induction programmes to integrate new staff and ensure resilience of the security infrastructure?	☐ Yes ☐ No
Do you have contingency plans? Do they include all anticipated scenarios?	☐ Yes ☐ No
Have you established formal arrangements with the escort?	☐ Yes ☐ No
Do you have a media communication plan to be activated in case of a security incident?	☐ Yes ☐ No

Questions for the Escort	
Do you believe a credible threat (theft or sabotage) exists to the nuclear material you escort?	☐ Yes ☐ No
Do you receive sufficient information on possible threats that could affect your mission?	☐ Yes ☐ No
Do you have formal and comprehensive agreements with transport stakeholders (nuclear operator, carrier, regulator, etc.)	☐ Yes ☐ No
Have you been involved in the preparation of the transport security plan?	☐ Yes ☐ No
Do you periodically exercise the transport security arrangements in coordination with other stakeholders?	☐ Yes ☐ No
Do you have an electronic tracking system that is independent from the carrier system?	☐ Yes ☐ No
Will you be able to immediately notify a continuously staffed control centre in case of an incident?	☐ Yes ☐ No
Do you have pre-determined criteria—for equipment failure, security incidents, staff issues or any interference with normal transport operations— to take action?	☐ Yes ☐ No
Do you have clear rules of engagement, adapted to various levels of threats?	☐ Yes ☐ No
Do you have the legal basis to perform all anticipated actions?	☐ Yes ☐ No
Are escort members also trained to use less-than-lethal options?	☐ Yes ☐ No
Are you confident with the transfer of responsibilities between the escort and potential external response forces if the security threat escalates?	☐ Yes ☐ No
Do you have communication means compatible with those used by other stakeholders potentially involved during a security incident?	☐ Yes ☐ No
Are you satisfied with the paramedic support arrangements?	☐ Yes ☐ No
Are all escort personnel adequately trained and equipped to react to all foreseeable situations? Are you ready to react to both low-level (protestors) and high level threats (terrorists)?	☐ Yes ☐ No
Do you have procedures in place to ensure an effective transfer of responsibilities between different jurisdictions (i.e. cross-border)?	☐ Yes ☐ No

Questions for the Regulator	
Does the legislation establish a regulatory organisation, independent from nuclear operators and carriers, to oversee transport security arrangements?	☐ Yes ☐ No
Have you established transport security regulations that are compliant with international requirements and recommendations? Do they include both prescriptive and performance based requirements?	☐ Yes ☐ No
Have you involved all stakeholders during the development of the regulatory requirements?	☐ Yes ☐ No
Have you identified and defined in the regulatory regime what transport information was sensitive and needed to be protected?	☐ Yes ☐ No
Have you identified all organisations that need threat information? Do you adapt your communication to various stakeholders? Is the threat assessment up to date?	☐ Yes ☐ No
For international transport, do you have mechanisms in place to exchange threat information with other countries?	☐ Yes ☐ No
Should there be a significant incident during transport, would you be informed in a timely manner?	☐ Yes ☐ No
Are you satisfied with the transport security skills and competences of your staff? Can you demonstrate their competence?	☐ Yes ☐ No
Are there regulatory requirements for relevant staff to be certified to hold positions with transport security accountabilities?	☐ Yes ☐ No
Do you have an effective inspection programme?	☐ Yes ☐ No
Are you requiring background security checks for staff holding positions with transport security accountabilities?	☐ Yes ☐ No
Do you have domestic and international mechanisms to ensure learning from experience (inspection, incident reporting, forums of exchange, etc.)	☐ Yes ☐ No
Do you have a media communication plan to be activated in case of a transport security incident occurring under your jurisdiction?	☐ Yes ☐ No
Have you established formal arrangements with other regulatory authorities for mutual assistance and benefit of sharing experiences?	☐ Yes ☐ No

APPENDIX B

DEFINING DIFFERENT LEVELS OF ORGANISATIONAL SUCCESS IN IMPLEMENTING A SECURITY PROGRAMME FOR TRANSPORT OPERATIONS (NUCLEAR OPERATOR)

The following chart presents five stages, each with its own set of characteristics, for developing and implementing an effective security programme for nuclear material in transport. By identifying where your organisation falls on this chart, you will know what you need to do to move to the next stage and improve your ability to secure the nuclear material being transported to and from your site.

LEVEL	CHARACTERISTICS
1 **RESILIENT**	The integrity of transported materials is seen as essential to the reputation of the organisation and senior management take a proactive interest in this area. Metrics and procedures are in place, and give very high assurance that an immediate response would be activated in the event of any unauthorized interference with the shipment. Relationships with other stakeholders, including regulators and armed response agencies, are excellent and communications and response arrangements are tested on a regular basis using realistic and challenging scenarios. Responsibilities have been agreed and documented in Memoranda of Understanding or comparable documents. The organisation receives permanent information on the location and status of the shipment and has a team on duty to immediately react in case of an incident. Individuals engaged in transport security have their competence certified and succession plans are established. The organisation is a leading actor in the transport security area and is consulted by its industry peers for advice and assistance.
2 **PROACTIVE**	Transport security operations are seen as an important operational issue by the organisation and the Management expects to see it performed competently and efficiently. State of the art security systems are expected to be used by the carrier. Threat information is regularly communicated to the organisation, which coordinates with other stakeholders for the preparation and conduct of transport. The organisation is involved in the design of the security plan and participates in table-top exercises to identify any logistical issues. Individuals engaged in transport security have been certified in their competence and the organisation follows developments in transport security regulations and technology with interest. The organisation receives frequent information on the location and status of shipments. Individuals dealing with the media in case of an incident are competent and a communication plan is ready to be activated.

LEVEL	CHARACTERISTICS
3 **COMPLIANT**	Senior management has interest in transport arrangements but investment in this area is seen as an unnecessary overhead to assure security. The organisation participates in a few meetings with other stakeholders when invited. There is a very basic process in place to learn from experience. Individuals engaged in transport operations have been trained but cannot demonstrate their competence for security. The organisation receives frequent information on the location and status of the shipment. Individuals dealing with the media in case of an incident receive awareness trainings.
4 **REACTIVE**	Transportation is managed by generalist staff that has limited experience in transport security operations. Senior management has limited visibility and interest in transport arrangements. The organisation only participates in meetings with other stakeholders when required by the regulator and does not use the threat information it receives. There is no process in place to learn from experience. Individuals engaged in transport operations have limited understanding, skills and competences for security. The organisation receives minimum information on the location and status of the shipment. Individuals dealing with the media in case of an incident have limited understanding of security issues.
5 **VULNERABLE**	The organisation has no interest in spending any more money on transport than is absolutely required. Senior management has no visibility or interest in the transport arrangements. The organisation does not participate in meetings with other stakeholders and does not receive threat information related to transport operations. Individuals engaged in transport operations do not have the necessary understanding, skills and competencies. The organisation receives no information on the location and status of shipments, beyond departure and arrival notifications. In case of an incident, multiple, non-coordinated individuals might be involved in communicating with the media.

ISBN: 978-3-903191-58-7
