Good Practice Guide

Nuclear Transport Security

Version 2.0

Why You Should Read This Guide

The transport of nuclear material is essential for the nuclear industry and is central to the nuclear fuel cycle itself. Protecting nuclear material during transport between locations requires effective cooperation and coordination between a number of different organisations often located in different countries.

The parties involved in nuclear material transports include the consignor (who sends the nuclear material), the carrier (who conveys the nuclear material), the consignee (who receives the nuclear material) and the competent authorities that have responsibility for approving the transport of nuclear material in their countries and throughout the world. In addition, guards, emergency responders, law enforcement agencies and other key organisations are involved. It is important that every organisation engaged in the transport of nuclear material has clearly defined accountabilities.

In some respects the management of transport operations for nuclear cargoes that require high levels of security due to the nature of the material can be more challenging than security at a nuclear facility. The circumstances during the transport of nuclear material are dynamic, and it is well acknowledged that nuclear material could potentially be vulnerable in transport. Special attention needs to be paid to security at all stages of the transport operation and in particular to the possible threats that could materialise during the journey. The development of a transport security plan (TSP) for the transport of high-consequence nuclear material is essential for documenting all security measures and arrangements that are required. Emergency response plans need to be available and rehearsed to prepare for any nuclear security incidents that may occur while the nuclear material is in transit.

As the transport of nuclear material takes place in the public domain — including over public roads and railways — effective planning, coordination and communication are essential to maintain public trust and confidence in this vital process. It is also important that the sensitive information about the movement of nuclear material is appropriately protected so adversaries with malicious intentions do not have an opportunity to use this information to plan an attack.

This guide has been produced to identify best practices and lessons learned from operational experience gained during the transportation of nuclear material classified by the IAEA as Category I and II or shipments of nuclear materials that may lead to high radiological consequences if subjected to sabotage (see IAEA NSS No. 13). It is particularly important that the State, its nuclear regulators, consignors, consignees and carriers work together to ensure that transport security arrangements are robust and that the response to threats is both effective and efficient. Carriers 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.

Aboui the Preparation of this Guide

In preparing this guide, we have taken note of the real-life experiences of organisations, including those that are transporting or protecting nuclear material in transport.

Wherever possible, this guide uses the same terminology as that found in the International Atomic Energy Agency (IAEA) Nuclear Security Series and Safety Series publications. These publications are commonly used as the basis for the legal and regulatory framework for the transport of nuclear material around the world. The guide takes into account the IAEA Nuclear Security Series Implementing Guide titled Security of Nuclear Material in Transport (NSS No. 26-G), which was published in 2015.

The preparation of this Best Practice Guide was supported by the US Department of Energy/National Nuclear Security Administration under Award Number DE-NA0003949 but the views expressed are those of WINS.

We Welcome Your Comments

We plan to update the information in this guide periodically to reflect best practices and new ideas. Therefore, we ask that you read it carefully and let us know how it can be improved. Please email your suggestions to info@wins.org. If you have ideas for additional WINS Best Practice Guides, we would like to hear about them. WINS is committed to working with nuclear security professionals; our objective is to share best practices to achieve operational excellence.

Mr Martin Porter
Secretary General
World Nuclear Transport Institute

Dr Roger Howsley
Executive Director
World Institute for Nuclear Security

WNTI Contact Information

World Nuclear Transport Institute
LABS, Victoria House, Bloomsbury Square,
London, WC1B 4DA, United Kingdom

Email: wnti@wnti.co.uk

Phone: +44 20 7580 1144

www.wnti.co.uk

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

July 2020
Version 2.0
ISBN: 978-3-903191-72-3
WINS (20)22

Contents

01

The Transport of Nuclear Material

Introduction

A wide variety of nuclear and other radioactive material has been transported safely and securely for many years to support the generation of electricity, the application of radioactive material in medicine and for other beneficial purposes. Over 20 million packages of radioactive material are transported each year – most contain small quantities of radioactive material for medical, industrial or research purposes. Civilian nuclear power and some military activities give rise to a relatively small number of shipments with significant amounts of nuclear material.

Only a small number of these transport operations are of nuclear material that require higher levels of protection for both safety and security reasons. In the civil sector, these are, for instance, shipments of spent fuel, of mixed oxide (MOX) fresh fuel assemblies, or plutonium to be used in the fabrication of MOX fuel.

The figure below 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 the transport of irradiated spent (or used) fuel directly from a power generation facility (item 6) to either storage or disposal facility (item 9).

The front end of the fuel cycle (items 1 through 5) typically involves the mining of uranium ore through refining, conversion and enrichment, followed by fuel fabrication.

More than 450 reactors are operating worldwide. Each of these reactors requires periodic deliveries of fresh nuclear fuel. These transports are typically classified as Category III or below (lowest security levels) based on the IAEA's guidance and are not the focus of this guide. However, some of the research reactors that produce radioactive isotopes for medical and other purposes are still fuelled with highly enriched uranium fuel (above 20% U-235 enrichment) and the power reactors that use MOX fuel, which contains plutonium, may require shipments of fresh nuclear fuel that would likely be either Category I or II (highest security levels) depending on the nature of the shipment and the amount of the fuel involved.

The back end of the fuel cycle includes operations concerned with the spent fuel discharged from 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).

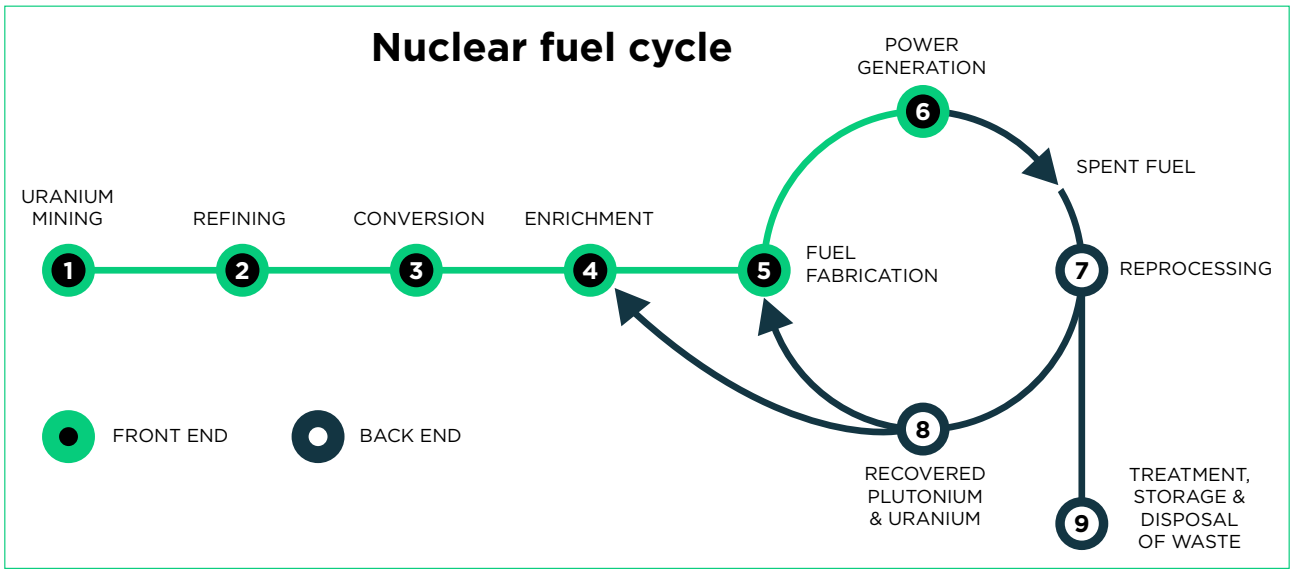


Figure 1: *The nuclear fuel cycle*

Movement of Nuclear Material

Shipment or transport of nuclear material can take place by different modes of transport. Nuclear materials may be shipped using five different modes of transport:

- Road
- Rail
- Maritime (oceans and seas)
- Inland waters (lakes, rivers, canals)
- Air

The mode(s) of transport chosen depends largely upon the country's geography and the ultimate destination of the nuclear material. For example, land-locked countries, such as those in Europe, will generally use road and/or rail. Larger countries, such as Kazakhstan, commonly use rail due to the vast distances involved. Coastal countries such as Sweden and Japan generally prefer maritime transports. Another important factor in relation to the choice of transport mode is public acceptance (or lack thereof) of certain transport options. For example, some communities do not accept the road transport of nuclear material through their towns and cities.

Different modes of transport require different considerations. Some specific ones for the shipment of Category I and II nuclear material, which requires additional security measures, are briefly set out below:

Road Shipments

Road shipments of Category I/II nuclear material are common. These materials are transported in specialised transport containers conveyed in high security vehicles (HSV). Typically, HSVs are escorted by other security vehicles dedicated to protecting the nuclear material during transport and to supporting the convoy, including by maintaining communications among vehicles and with the transport control centre.

Rail Shipments

Rail is used extensively in certain countries for the movement of nuclear material. For example, in the UK rail has been used extensively to transport spent fuel to reprocessing and interim storage facilities as well as for the consolidation of nuclear materials between nuclear facilities.

Maritime Shipments

Generally two types of ships transport Category I/II nuclear material 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.

- Other vessels, typically used for longer sea voyages, are constructed so specially designed shipping flasks can be 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.

Inland Waters (Lakes, Rivers, Canals)

Inland water transports are usually undertaken using small vessels and/or barges. The use of inland waterways can provide a useful alternative to road or rail, particularly when longer transports are necessary, and it is becoming a more common in Central Europe and other land-locked regions.

Air Transport

Civil movements of Category I/II nuclear material by air are less common, because of the size and weight of the transport containers (nuclear material cargo), although a number have taken place. For example, between 2016 and 2019, nuclear material was flown from the Dounreay nuclear facility near Thurso in Scotland to the USA in a series of flights using military aircraft. Planning for such movements is a highly complex process involving a range of stakeholders, including government officials, regulators, consignors, carriers, consignees, and civil aviation authorities. It is more common for other radioactive material such as short-lived radioisotopes used in medicine to be transported by air. All civil transports by air take place under the Convention on International Civil Aviation, commonly referred to as the Chicago Convention and in accordance with ICAO's Technical Instructions, which incorporate the recommendations of the UN Model Regulations. Further to this, national legislation and regulations may apply to air transport movements; for example, the Nuclear Industries Security Regulations 2003 sets out the requirements in the UK.

02

International Framework and National Regulatory Considerations

International Recommendations and Guidance

As many elements of the transport of nuclear material are international, it is not surprising that the Convention on the Physical Protection of Nuclear Material (CPPNM) was originally drafted to cover the international transport of nuclear material. The CPPNM was the first legally binding international instrument relating to physical protection of nuclear material. The obligations of States Parties, those countries that have signed the convention, include the protection of nuclear material during international transport.

In 2016, an amendment to the CPPNM entered into force. The amendment expanded the obligations of States Parties to the CPPNM who ratified the amendment. These expanded obligations include the requirement to ensure physical protection of nuclear material in domestic transport and protection against the sabotage of nuclear material in transport.

Another international instrument that is very important but not legally binding is the IAEA Nuclear Security Series No. 13 (INFCIRC/225/Rev 5). This document provides recommendations to States on how to establish, maintain, and sustain an effective physical protection regime for nuclear facilities and for nuclear material, including during the transport of nuclear material. It also has important guidance for countries that are not State Parties to the CPPNM but either are responsible as consignors, consignees, or carriers of nuclear material or are a country through which nuclear material may transit and want to demonstrate an appropriate level of protection.

The obligations of States Parties to the CPPNM as well as the recommendations and guidance in the IAEA Nuclear Security Series is used by States as a basis for their national legislation and regulations. These documents provide support to regulators, operators and carriers in relation to the secure transport of nuclear material. In particular NSS No. 26-G provides additional guidance on how to implement in practice the recommendations on the physical protection of nuclear material contained in NSS 13.

There are a number of international organisations that have responsibility for the international framework for the different modes of transportation in relation to dangerous goods. The overarching framework is the UN Recommendations on the Transport of Dangerous Goods Model Regulations (the Orange Book). The Model Regulations on the Transport of Dangerous Goods presents:

> ***a basic scheme of provisions that will allow uniform development of national and international regulations governing the various modes of transport; yet they remain flexible enough to accommodate any special requirements that might have to be met. It is expected that governments, intergovernmental organisations and other international organisations, when revising or developing regulations for which they are responsible, will conform to the principles laid down in these Model Regulations, thus contributing to worldwide harmonisation in this field.***

This is then subject to specific additional guidance from the relevant international organisations concerned with the different modes of transport, including aviation (ICAO and IATA), maritime (IMO), rail and inland waterways.

Regulatory Framework for Transport Security

The creation of a national legal and regulatory framework for nuclear security is the responsibility of individual States. Those involved in the transport of nuclear material (consignors, carriers, consignees) need to ensure full compliance with all regulatory requirements. Performance based approaches to regulations allow more flexibility in developing and applying security measures and often lead to more effective and resilient security arrangements.

The regulatory oversight for secure transport of nuclear material will be undertaken by one or more independent competent authorities. In some States this may be a combination of a transport competent

authority and the nuclear regulatory body. In other countries the nuclear regulatory body is also the competent authority for the transport of nuclear material. Regardless of the specific regulatory framework that may be in place in a country, it is the responsibility of the consignor, consignee and carrier to ensure that they comply with all regulatory requirements.

The regulations for the secure transport of nuclear material are developed taking into account the quantity and the physical/chemical form of the nuclear material and the type of packages being used for the transport of the nuclear material.

It is good practice to involve all stakeholders, especially nuclear facility operators and transport carriers, during the development of regulatory requirements. In some countries this is done through a consultation process that is mandated as part of the development and introduction of new regulatory requirements. In addition some countries have a formal process to assess the impact of new regulations on industry (called regulatory impact statements). Regular consultation between industry and the competent authorities can be beneficial in this respect.

Good Practice: Where possible, nuclear security regulations should be performance based rather than based solely on prescriptive rules. This is particularly important for Category I and II shipments or those that may lead to a high radiological consequence if subject to sabotage during transport. Adopting a performance-based approach will provide the operator with greater flexibility in developing security arrangements that fit their organisational needs and enables them to deliver robust, credible arrangements that ensure accountability for effective security implementation rests firmly with the facility operator/carrier. It also provides additional assurance to stakeholders that the security measures deployed will protect the shipment in the event of a nuclear security incident.

International Considerations

When the consignor and consignee are within the same jurisdiction and legislation (i.e. within the same State), transport of nuclear material is generally less complicated than when nuclear material is transported through different jurisdictions and therefore subject to a number of separate national legal and regulatory frameworks.

Where there is a cross-border transfer of responsibilities for the nuclear material, responsibilities for the security arrangements must be discussed and agreed in advance between the two (or more) 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 of the nuclear material, including such matters as:

- The sharing of threat and risk information to enable the transport route to be planned and agreed
- Responsibility for updating the threat assessments during the transport of the nuclear material
- Assurances relating to the trustworthiness of personnel involved with the transport of nuclear material
- Arrangements for the maintenance of tracking information to ensure that the location of the nuclear material is known throughout the shipment (transport), where agreed
- Provision of secure locations for any scheduled or unscheduled breaks for the carrier and the personnel of the carrier
- The handover arrangements of the shipment between armed personnel and other escorts, including safety and medical support
- Coordinating the release of information about the transport of nuclear material both before, during and after the shipment

Good Practice: States Parties to the CPPNM should understand their legal obligations under the CPPNM in relation to international coordination of the shipment. Therefore, once it is known a transport is taking place, it is good practice for the States concerned to meet as early as possible in the process to discuss and agree on any potential problems that could arise in relation to security responsibilities, legal matters, communications or issues of any other planning nature.

Capturing and recording the agreement reached between the involved States on the transfer of security responsibility is a key aspect of any international shipment of nuclear material. Early engagement between all of the affected parties is important. How security responsibility will be transferred from one State to another should be signed off by the competent authorities or other government representatives from all of the States that are responsible for regulating and supervising the transport of nuclear material. Any proposed external release of information should also be coordinated and synchronised by the States involved. Agreement on what information about the transport operation will be disclosed and coordinating and synchronising entities that will make any announcements about the shipment is also critical.

CASE STUDY

An example of where communications can pose challenges was demonstrated in a recent shipment of nuclear material to a landlocked country. During planning, a transit State (a State through which the nuclear material is transported but is not the final destination) indicated its intention to release information about the shipment on arrival in its territory to reassure the public it was merely transiting through the country, rather than being the final destination for the nuclear material. However, the release of public information about the shipment would cause the consignee (the State receiving the nuclear material) problems due to political and socioeconomic sensitivities over the shipment. This is one example that highlights the need for all parties involved in the shipment to agree proactive and reactive communications well in advance of shipments.

Roles and Responsibilities

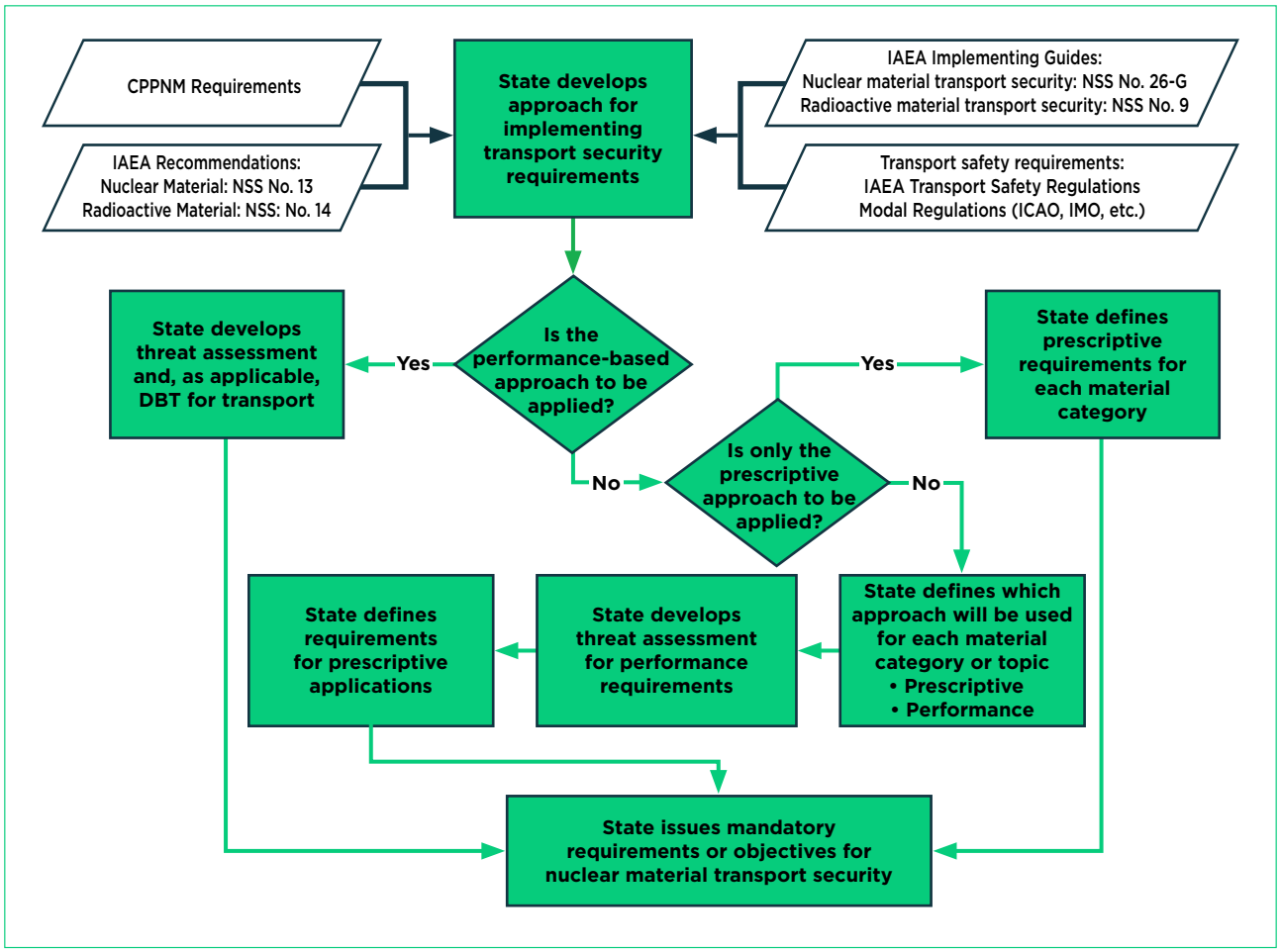
Identifying Roles and Responsibilities

Responsibilities for planning and implementing transport security will be assigned by the State and its competent authorities through the legal and regulatory framework for the transport of nuclear material. This will vary between States. The flowchart below (taken from IAEA NSS No. 26-G) demonstrates how to determine the regulatory process for transport security and how each State may issue requirements and/or objectives to those responsible for undertaking nuclear material transports. This may be in the form of a performance-based approach to regulations, a prescriptive approach or a combination of both.

The regulatory framework of each State will assign the responsibility for security to the parties. This is typically the consignor or carrier. For Category I and II shipments of nuclear material, this will generally include the requirement to develop a transport security plan (TSP) (see relevant section below). The consignor or carrier is also responsible for providing the consignee with all relevant information, such as the advance notification of shipments and expected time of arrival. It also has the duty to inform the consignee of any subsequent changes to this information.

Consignors need to ensure that any carriers assisting in the shipment are authorised to transport the particular category of nuclear material. Prior to the transport of the nuclear material commencing, the consignor and carrier should ensure that all the necessary permits and authorisations have been obtained; including the prior approval of the TSP. Also, before commencing the transport, the consignor or carrier should verify that all the security arrangements detailed in the TSP are in place or will be in place prior to the shipment. Any serious shortfalls may require the shipment to be delayed or, in the worst-case scenario, cancelled. This requires the oversight of the relevant competent authorities who have the legal responsibility for regulation of the transport of the nuclear material.

The consignor or carrier conducts an inspection of the conveyance (the vehicle or vessel that is carrying the nuclear material) prior to commencing transport; where practicable after any stops (scheduled and unscheduled); and on arrival at its destination. Inspections are carried out to determine



whether there has been any loss of or damage to or tampering with transport packages (nuclear material cargo) during transport or on delivery. The consignor or carrier will also inform the consignee (or other designated responsible organisation) of any unforeseen changes to the expected time of arrival. During the transport of nuclear material, the conveyances are continuously monitored to enable the consignor or carrier to respond to any security incidents along the route.

The consignee must be prepared to secure the shipment of nuclear material on its arrival and have appropriate personnel available to receive the nuclear material at a prearranged place, date and time. The consignee must also report to the consignor and/or carrier that all packages have been received intact or immediately contact the appropriate response organisations and the competent authorities if any problems are detected at this point.

Regulators and practitioners both emphasise that the development of 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.

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.

Skills and Competencies

All personnel involved in the transport arrangements and security should be 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 implementation of the security arrangements, and demonstrate that personnel are knowledgeable and competent. In some States, and for some positions (such as a Ship's Security Officer), there are specific regulatory requirements for relevant staff that hold security positions and who have managerial accountability to be certified. (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 of training records to consider whether the security personnel involved were suitably qualified and competent to carry out their role. It also makes good sense operationally. Where staff turnover is high, staff often will not have time to receive comprehensive and timely on-the-job training, so they need to be given structured training before taking up their responsibilities.

Good Practice: It is good practice for organisations to maintain a competency framework which enables them to provide a complete overview of organisational competency. Competency frameworks should be developed for all individuals who have a role in the secure transport of nuclear material.

03

General Considerations for Transport Security

Implementing a Graded Approach

One of the most challenging aspects of implementing effective security measures in general is to know how much security to apply. Too little security leaves nuclear material vulnerable, but too much security wastes money and could unnecessarily impact on transport operations without any reduction in risk.

Operators need to adopt a graded approach to security. A graded approach means applying resources and systems to security arrangements based on the threat to the nuclear material and the likely consequences if the threat materialises. The graded approach applies not only to the physical security measures implemented during the transport phase but also to other elements of the entire security programme, including information security and training and exercising requirements.

The competent authority and the facility operators and carriers need first to understand the potential forms of attack on the nuclear material during transport and consider whether the nuclear material being transported is principally at risk from theft of the material, sabotage or both. They must consider not only the potential radiological contamination of the surrounding area in case of a sabotage but also if the material could be stolen and used for malicious purposes in another location.

Categorisation of Nuclear Material for Theft

The starting point for designing security measures and deciding on the security arrangements to apply to a transport of nuclear material is to categorise the nuclear material being transported. The following categorisation table is based on Annex I to the CPPNM and sets out the different levels of requirements for the physical protection of nuclear material against unauthorised removal. The categorisation ranges from Category I (highest security level) to Category III (lowest security level, other than uncategorised material (some States define uncategorised material within national tables as Category IV)).

MATERIAL	FORM	CATEGORY I	CATEGORY II	CATEGORY 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% U-235 or more • uranium enriched to 10% U-235 but less than 20% • uranium enriched above natural, but less than 10% U-235	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/]	

[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 1 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 1 metre unshielded.

Factors other than nuclear material category may need be taken into account to ensure an appropriate level of security is applied. The chemical and physical form of the material has a significant impact on the attractiveness for theft to an adversary and is therefore worthy of consideration during this process. Material in a dilute form will force an adversary to acquire much larger volumes and masses in order to obtain a significant quantity, therefore, consignors may consider dilution during the categorisation process to reduce the level of security required i.e. a lower level. For example, plutonium contaminated materials may require a lower level of security than plutonium powders even though both transports may contain a similar amount of plutonium. Conversely, the total amount of nuclear material contained in a single shipment should be added together or aggregated when assigning security levels designed to prevent the theft of nuclear material. In doing so, the amount of material an adversary could credibly collect and remove in a single attack scenario on a shipment should also be taken into account.

Sabotage Considerations

Levels of security applied to transport were historically based on the categorisation of the nuclear material for use in the construction of a nuclear explosive device. More recently, an increased focus has been placed on the potential for the sabotage of nuclear material during a shipment and additional security measures above and beyond those applied for theft might be required to mitigate that risk.

As an example, following the guidance provided by IAEA NSS No. 9, a Category III cargo of plutonium powders would not normally require an enhanced level of physical protection based on its categorization, but if that cargo were sabotaged, it could result in the release of the plutonium powder from its transport cask or container and result in unacceptable radiological consequences. Therefore, the cargo would present a sufficiently high risk to require increased security measures.

The overall aim is to categorise nuclear material for theft but also take into account the potential for sabotage and apply the higher security requirement to the shipment, as appropriate.

Defence in Depth

Supporting a graded approach is the concept of defence in depth, which is common in the nuclear safety and radiation protection fields as well as in security. In safety analysis, the concept refers to creating multiple, independent and redundant layers of defence to reduce the likelihood of accidents.

In security, the concept refers to creating multiple, independent and redundant layers of defence to reduce the likelihood of a successful malicious act. It typically includes a combination of security equipment, procedures and administrative measures.

The concept of defence in depth is common on nuclear sites. For example, on the perimeter there may be external patrols, a perimeter fence with CCTV cameras and a detection system, along with an access control point. There may be one or more security fences inside the facility with security systems and associated access control points. Finally, the nuclear material may be stored in a strong room inside a secure building.

Examples of defence in depth in transport security operations might include forward covert patrols to carry out surveillance of the route; a robust, specially designed and built transport vehicle to withstand threats that may have been assessed as design basis threats; multiple independent physical barriers such as packages, containers or other over-packs; multiple locking devices; a driver accompanied by an escort in the cab of the vehicle; and a police escort consisting of multiple vehicles, both in front of and to the rear of the transport vehicle or convoy. If a malicious act were attempted during the transport, then these multiple, independent and redundant security measures will help to reduce the likelihood of success of the adversary

Good Practice: The concept of balanced security is also important; for example, using high security locks on a load carrier that has flimsy canvas sides is not balanced security. There is also little point in applying expensive physical measures (e.g. attachment points and tie-down attachments equal in quality and strength to the locking mechanisms) when effective trustworthiness checks on transport personnel have not been done or sensitive movement information has not been adequately protected.

Security by Design: Package and Conveyance Design

Transport containers used for the shipment of spent fuel, high-level radioactive waste, and MOX are typically known as Type B packages. This means that they are packages designed for the transport of fissile material. Such containers must pass performance standards derived from the IAEA publication 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.

Although packaging for nuclear material is generally very robust, is subject to stringent safety testing, and will therefore provide a level of protection against the threat, it should not automatically be assumed that packages which are designed to protect

material in the event of safety event will provide sufficient protection against a malicious act such as an attack with a stand-off weapon such as a rocket propelled grenade. It may not be possible to fully eliminate all risks and protect a nuclear material shipment solely through physical protection of the package or transport in general, but knowledge of the potential vulnerabilities from sabotage threats will enable planners to consider whether or not a particular risk is acceptable and/or influence response force tactics and security plan arrangements. Consequently, it is advisable to consider some form of testing, either real time, through simulation, or by expert opinion, to provide best estimates on the protection offered by a particular flask or security container against the various postulated threats.

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 to provide sufficient delay for a response. For example, over-packs may be made from high-security materials to protect against theft/sabotage, be fitted with secure tracking devices and have double high-security locking mechanisms. In common with nuclear facility security, designing security into the transport vehicles and associated equipment to enhance their resilience has advantages. For example vehicle cabs may be ballistic proof, fitted with immobilisers and secure tracking, and use biometrics for identification purposes.

Safety and Security Interfaces

Safety and security intersect on transport operations, the assets used and arrangements adopted. Understanding the interface between safety and security, and recognising opportunities to exploit synergies between the two, is critical to nurturing a culture of harmonised security and safety. Flexibility is the key to ensuring a balance is reached, and this requires negotiation, cooperation, patience and understanding between representatives of the two disciplines. Experience shows that this is always possible to resolve or manage any conflicting issues that may arise.

The following paragraphs discuss examples of interfaces, possible challenges and potential synergies between safety and security:

- The robustness of a transport package can provide a certain amount of security, as the package can provide a degree of protection against forcible attack and/or an element of ballistic protection. The sheer physical weight of many packages also means they cannot be easily transferred from one transport vehicle to another without special lifting appliances. In this regard the safety features may support the security objectives

- Transport regulations usually 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, labelling conveyances in this way attracts undesirable attention to the shipment. If alternative measures acceptable to the transport safety competent authority are in place, such as such as emergency response personnel accompanying the shipment and specific communications arrangements, external markings may not be necessary.

- The speed with which the transport operation travels is also an area where there may be different views. For security reasons, where the threat and other factors dictate it is the best option, 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 low speeds and frequent breaks to rest the transport crews and check safety systems.

Developing a Transport Security Plan

Category I and II nuclear material shipments require the development and implementation of a transport security plan (TSP) that serves as a roadmap for all stakeholders involved in the shipment and is subject to regulatory review and approval. The plan describes risk in terms of the categorisation of the shipment for theft and sabotage, any potential vulnerabilities and the security measures required to prevent or mitigate these vulnerabilities. It also demonstrates how the various security systems achieve the required security objectives of deterrence, detection, delay and response. The plan also identifies who has overall responsibility for transport.

Having a comprehensive TSP helps the carrier prepare and respond to any unexpected incidents that might happen during a transport and minimise risk to employees and the public. Carriers engage early with all stakeholders involved to ensure plans are integrated and that any transfer of security responsibilities is clearly defined in the documents. The plan also includes a range of contingency plans to cover all potential eventualities.

Usually no single document can consolidate all transport security-related information. TSPs are the central piece of the security documentation and need to be structured around key areas and refer to lower-level documentation that can be reviewed independently and in some cases be compartmentalised to reduce the risk that the plan is lost or compromised.

TSPs may be generic in nature and applicable to a series of similar transports (approved accordingly by the regulator) or may be specific to one transport. Where generic plans are used, learning from experience and amending the plans where considered necessary is important.

Carriers should ensure that the entire set of documents that comprise the TSP have appropriate protective marking and that the entire plan 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 organisations that are located in other countries and may not be subject to the same requirements for information classification and protection.

Where no national protocols exist in this area, carriers should include the protection of sensitive information in the contractual conditions.

Good Practice: Taking an inclusive approach to the development of a TSP is good practice. The security team may lead on the development of the plan, but the arrangements need to work for everyone and consequently a range of stakeholders should provide input into the plan and/or review its contents. This does need to be balanced against confidentiality issues, as the plan will include sensitive information. However, here compartmentalisation of the plan may be considered to ensure the need-to-know principle is applied.

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. Detailed threat assessments 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). The State will likely define a baseline threat assessment that can be used for planning purposes and reviewed/updated before the TSP is approved.

The accountabilities for assessing the threat should be clearly defined in the national legal and regulatory framework and reflected in the planning documentation since this forms an essential component of the risk assessment associated with the transport operations. Carriers 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 and mechanisms to share threat information related to the transport route. Agreements will need to be reached between States on how this is best achieved so all parties have confidence in the planning process.

Vulnerability Assessment

The approved TSP needs to demonstrate how the effectiveness of the security arrangements has been validated. This is generally done through performance-based testing. This could comprise one or more proven methodologies such as force-on-force exercises, tabletop exercises, war gaming, simulation, computer-based modelling and/or expert analysis. These methodologies are primarily used to carry out vulnerability assessments on nuclear facilities but can equally be applied to the transport of nuclear material. Vulnerability assessments should be based on the design basis threat (DBT)/threat assessment and are most likely to be sensitive and classified. They are designed to identify weaknesses in the security system/arrangements that could be exploited by an adversary and determine how the human, procedural and technological elements of security systems may be expected to perform against attack as postulated in the DBT/threat assessment.

Good Practice: Developing credible, consistent and challenging scenarios is good practice to predict the methods that could be used by attackers and to help ensure that the security systems are effective against the postulated threats. Scenario analysis is important and provides a basis for the confident evaluation of the security arrangements. Scenarios should be documented and consistent with the DBT.

Where the vulnerability assessment identifies any potential shortcomings in existing or proposed security arrangements, additional security requirements or arrangements may need to be applied to the transport or other solutions may be considered such as changing transport modes, routes or even splitting the shipment into smaller shipments to lower the category/potential consequences of each movement.

Modelling and simulation techniques are 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 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. Adoption of an all-hazards approach to risk analysis is considered best practice.

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 lace. Exercises can take a variety of forms; best practices for such exercises are reviewed in WINS' International Best Practice Guide on Security Exercises (see Further Reading). It is essential that exercises are as realistic as possible and challenging. The scenarios must be capable of establishing whether or not the plans are resilient, and ideally the exercises should involve the different agencies and personnel that have accountabilities for the transport of the nuclear material.

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 used to validate and test the security plans/procedures, provide a learning environment, and develop staff competencies and teamwork.

Some organisations use 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 avoiding false confidence in the arrangements is, 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.

Good Practice: Using the information from your DBT and vulnerability assessments will allow you to develop a range of scenarios on which to test your organisational capacity. Over time, you should try to make these more complex and stretch your arrangements, procedures and people. The culmination of this graduated approach may be a force on force exercise or a real-time exercise that takes place over a number of days to test both your response and recovery.

Personnel Reliability

Implementing effective security during transport requires both the transport and security systems and the personnel associated with the transport to be reliable. These personnel should display the honesty, integrity, and values necessary for employment. All personnel involved with transportation of nuclear material requiring a high level of security should undergo background security checks (reliability assessments) commensurate with their responsibilities including their access to sensitive or classified information and material. This is necessary to ensure a trustworthy workforce and minimise the possibility of insiders becoming nuclear security threats. Such checks need to be completed in advance of transport operations and should be reviewed periodically.

The nature of transport operations means that many different personnel may have some ancillary involvement with the operation, including port workers, maintenance engineers 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, escorting, searching and security inspections and checks before departure as well as measures to ensure continuity of knowledge concerning the integrity of the consignment.

Good Practice: Reliability checks are often focused on those who are directly involved in transport operations. However considering those who might be involved indirectly, such as those involved in booking pilots for marine port arrivals/departures, the provision of catering, etc. is important. Whilst it might not always be possible to confirm the reliability of these individuals, there are ways to reduce their knowledge of the shipment and minimise the time they aware that a shipment may be taking place. Further information can be found under Information Security.

Continuity of Personnel

Personnel responsible for high consequence nuclear material transportation security 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.

Information Security

The security of information is essential to maintain the security of nuclear transport operations and to ensure public confidence. Therefore, to operate effectively, consignors and carriers should maintain the confidentiality, integrity and availability of sensitive transport information. Information and associated assets comprise data in various formats, such as digital, hard copy and knowledge, as well as information technology and operational technology equipment or software.

When developing their regulatory framework for information security, States should identify and define which transport information is sensitive and needs to be protected. For example, the quantity of nuclear material, routes, dates, times, locations, and details of guard/response forces are all very sensitive, as they might enable an adversary to plan an attack. However, consignors and carriers must be able to plan and share plans effectively. Maintaining confidentiality is difficult when information needs to be provided to a range of stakeholders. Where information sharing is required, the use of date codes, predeterminations of trustworthiness, compartmentalising information and the need to know principle together may help maintain confidentiality. Sharing sensitive information between States requires further considerations, as they will have their own arrangements for protecting classified information. Formal agreements may be needed before certain information is passed between States.

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

Good practice for information security includes:

- Avoiding blanket classifications – documents and information related to transport operations should be classified on the basis of their specific and individual 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 who may not be authorised to receive the information.

- 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 people may take an interest in and monitor transport operations. If this is the case, operators can lose credibility if they 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 include 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.

- Information 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 security arrangements for transport 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.*)

Route Selection

For road transports differing routes may be 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. For example, bridges may have weight or height restrictions. The journey time also has to be considered. One of the common requirements in NSS No. 26-G is to "minimise the total time during which the nuclear material remains in transport"; however, the shortest route may not be the most secure as it may transit through areas of potential unrest or natural faults. There may be other reasons why the shortest route is not the most secure. The response time to an incident on a particular route should also be considered.

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 in the deep sea may be considerable. This needs to be factored into the security arrangements for the cargo so adequate protection and delay are provided. For high consequence shipments of nuclear material, this may mean an armed guard/response force will be required to accompany the shipment either on the load carrying vessel or an escorting vessel.

For maritime transport in coastal waters, a vessel is more restricted by navigational constraints such as

draught, water depth, navigational marks, navigation separation zones, land, islands and other shipping. More shipping traffic is likely 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.

Numerous examples worldwide show conflicts exist between commercial and security interests; for example, taking a longer route incurs more cost. The ultimate aim should be to meet the required security objectives. Objective setting regulation rather than prescription can help the carrier to meet objectives and operational needs whilst keeping costs to a minimum by designing their own security arrangements.

Land Transport 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. Where this is not possible, establishing a temporary protected area should be considered by the deployment of additional guard/response forces or the deployment of temporary physical security measures. The transport control centre must be kept informed of arrival and departure at planned stopovers.

A transport may be forced to make an unplanned stop, for example due to a mechanical fault with a vehicle in the convoy. The transport control centre must be immediately informed of any unplanned 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 defined in the TSP and exercised. Where this is for a protracted period, as far as is practicable, a temporary protected area should be considered.

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 needed when material is transferred to ensure a commensurate level of protection is afforded at all times. 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 strictly controlled and limited to the minimum number of personnel necessary to conduct the transfer safely and securely. The use of temporary physical and technical security arrangements may also be considered, such as the deployment of temporary vehicle barriers and fences. Inter-modal transfers usually also include a range of suppliers, which can create additional information security challenges to balance of confidentiality and availability of information.

Good Practice: When dealing with multiple stakeholders and suppliers, one useful tip is to share sensitive details as late as is reasonably possible in the planning process. This will reduce your risk by minimising the opportunity for a threat actor to prepare and launch an attack.

Preventing Gaps and Overlaps during Handover

Avoiding gaps and overlaps in accountability during the handover of responsibilities is important. Particular attention needs to be given at this time to regional or national boundaries and different organisations (such as a reinforcement team). In areas such as harbours, 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 dialogue between the various parties, written agreements on accountability, and joint exercises that test the arrangements in practical and realistic settings. Avoiding overlaps in responsibility is just as important as avoiding gaps in responsibility.

04

Transport Operations

Key Considerations

Nuclear material should only be transported outside of nuclear premises when absolutely necessary. All transport journeys should be as short as possible (commensurate with safety and logistical considerations). Occasionally a longer route may be more secure, for example, moving nuclear material by sea along a coastline rather than by road or rail. The number of intermodal transfers should be kept to the minimum required.

All transport journeys should be preceded by appropriate security planning and notifications, and movements should be co-ordinated with relevant agencies and organisations. Contingency plans should be prepared and practised to ensure that appropriate procedures can be implemented in response to a reasonably foreseeable incident, including unplanned stops.

Nuclear material in transit should never be left unattended. All nuclear transports should be appropriately tracked to enable its location to be known at all times.

Nuclear transportation should be appropriately protected through a graded approach. Security measures should be designed considering the principles of defence in depth. Security measures should be based upon an appropriate DBT or threat assessment including appropriate measures to deter, delay, detect and assess, and respond to (4D+R) any malicious activity (including insiders). Nuclear material in transit should not be unnecessarily exposed to known human hazards such as civil disturbances.

Information relating to the movement of nuclear material should be appropriately protected and shared on a need to know basis. Whenever possible, no patterns relating to routes or timings should be established. Operational technology associated with the movement of nuclear material should also be appropriately protected from compromise.

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. Therefore they should form part of the quality management arrangements. Checks should include all administrative, personnel and equipment components, and they should identify any deficiencies and required corrective actions. If correcting any identified deficiency prior to a planned transport is not possible, carriers should take advice from their competent authorities as to whether the transport can take place or if it needs rescheduling.

Monitoring and Tracking Shipments

To enhance security and monitor the nuclear material shipments, remote electronic tracking and monitoring systems with secured communications should be used for all Category I/II and other high consequence shipments. If applied effectively and integrated successfully into a proper transport control system appropriate to the particular nature of the consignment, such systems can provide an added layer of security and functionality. Properly configured they can also provide early warning of unauthorised activities and movements, thereby allowing activation of a timely security response.

An electronic tracking system can provide instant and automatic alert/alarm notification to support incident response and emergency management arrangements. 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. Monitors will know where the alert is coming from and 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.

The electronic tracking device should be fixed to a conveyance (e.g. rail car, lorry cab, ship) or package to visibly track materials while they are in transit. Electronic tracking commonly uses the Global Positioning System (GPS) and a satellite communication or cellular general packet radio service (GPRS) working together to provide and transmit information.

Good Practice: A key question to address is the decision on which item to track. For example should the tracking system be fitted to the package (which could potentially be lifted from the conveyance) or the conveyance (which could be driven off with the package)? For higher consequence shipments, it is good practice to consider fitting tracking to both the conveyance and the package and report separately the alarms generated by the system.

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. The centre for monitoring and communication plays an extremely important role supporting 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.

Training will be required to ensure accurate and timely interpretation of the tracking data. Those with access to the data must be equipped with encryption devices—perhaps manual keys or equipment that generates ephemeral keys of codes of short duration. These systems are able to identify and authenticate legitimate data users.

Command and Control

The transport of nuclear material takes place outside protected facilities, often distant from commencement of the transport operation and across multiple jurisdictions and State borders. This means that multiple local law enforcement and emergency response agencies may be involved, as well as multiple State competent authorities for international shipments. Consequently, an agreed and well-defined plan for command and control in a nuclear security incident involving transport must be in place to ensure all stakeholders share the same objectives and clearly understand their roles, responsibilities and authorities.

The term *command and control* may mean different things to different communities, so it is important to understand that different approaches to accomplishing the functions of a command and control operation exist. 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 to eliminate doubt as to what they are in the lead-up to an incident, during an 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 of 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? The primacy of response will be determined by the nature of the emergent threat. If time permits a multi-stakeholder tactical coordination group within the transport coordination centre will determine possible courses of action; however, if an immediate threat to life or cargo is presented on the ground, the escort commander must have the

contingency procedures and rules of engagement in place to be able to react and deal with the threat.

In the case of a maritime shipment, do they fall under the Ship's Master? All personnel embarked in a vessel fall under the responsibility of its Master and this includes the delivery of armed escorting effect. Operating procedures designed by the carrier and based on the perceived threat assessment and DBT of the flag under which the vessel is sailing guide the Master on their response.

Do they have the power to take whatever actions they deem necessary? In any event and as per the agreed rules of engagement, most escort teams reserve the inherent right to self-defence and may fire to defend themselves and the cargo without reference to the Master.

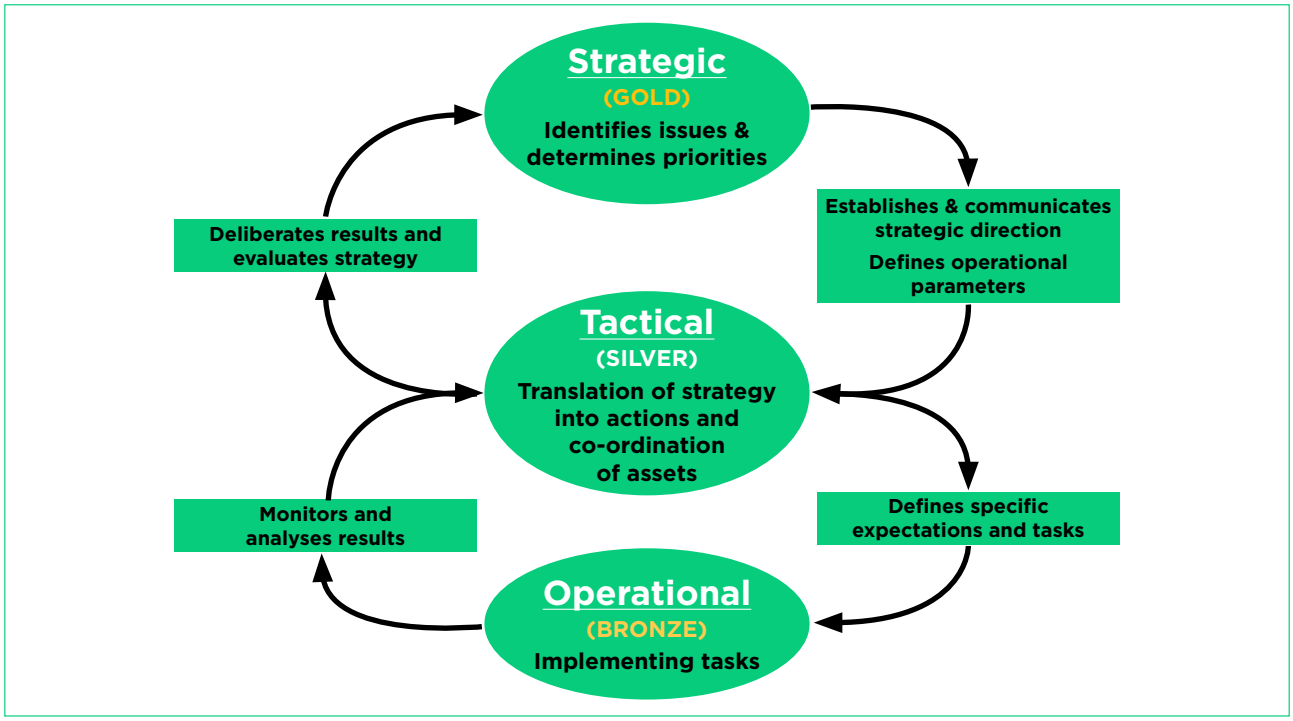
If additional forces arrive to reinforce the convoy, do the armed personnel become subject to the command of the incoming force? The interoperability of participating armed forces is established very early in the transport planning cycle. Well understood operating procedures, areas of responsibility and handover are agreed both at the strategic and tactical level so as to avoid any doubt during transport operations.

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.

The transport control centre is the logical central location from which to direct a response. It should continually track the current position, monitor security status of the shipment, and alert response forces in the event that a malicious action is threatened/occurring/has occurred. The gold silver bronze (GSB) structure supports this framework for delivering a strategic, tactical and operational security response to a malicious incident or operation.



Response to Incidents and Crisis Management

Contingency Plans

Any comprehensive transport security system should include contingency plans to address how anticipated and unanticipated security events are to be handled and how authorised persons should prepare to respond to a nuclear security incident at the local, national and international level. These contingency plans should be included or referenced in the TSP.

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 they should be rehearsed and reviewed as many times as required. The contingency plans should include performance indicators to assess whether the required outcome is being achieved.

In addition to general contingency planning for the shipment, the response force may have an organic and comprehensive set of operation orders for each transport. Carriers and response forces should engage early to discuss and agree on the TSP, contingency plan, and response force operation order content, as full alignment at all times between these documents is imperative.

Arrangements for dealing with protest action should be considered (along the route or at trans-shipment points) in advance as part of the contingency planning 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.

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 any subsequent decisions that are made will have an important influence on the planning and response arrangements. Such issues need to be considered by the relevant parties during the planning phase and agreement reached on the optimal arrangements.

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.

Private organisations offering armed escort and protection measures exist, inclusive of maritime shipments (largely in response to the high incidence of maritime piracy in recent years). Use of such organisations depends on the jurisdiction that applies; the transport route may not be not supported or approved by all participating countries.

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

Co-ordination between Escort and Response Forces

A clear definition of command and control is needed 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, the chain of communication between the two command structures must be well established. The change of responsibilities must be exercised so it is seamless and clearly defines who is in command of the situation at a particular time should an event occur. Furthermore, 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 (RoE) and the appropriate use of force. Nevertheless, international standards should also be considered when determining 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) justifies different RoE from that employed 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 would ever reasonably justify a different approach to the use of force when compared to that 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 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 obtain sound legal advice before any shipment involving armed guards takes place and that the training and tactical planning is in accordance with that advice.

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 a strategy and identified spokespersons need to be agreed. If an incident occurs that involves the deployment or use of firearms, most attention will be on that aspect of the incident. The security manager or armed force commander needs to 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 response force been consulted on the aspects relevant to them?
- What are the mechanisms for ensuring that references to the armed response force and their work do not risk compromising the current operation? Media coverage could have the potential to compromise security arrangements 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? The media is likely to demand reassurance that 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 the benefits to investing time briefing 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.

05

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 the 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. A spirit of continuous improvement within the organisations and constantly pursuing more effective and efficient ways to improve the transport operations is crucial.

Learning from Experience

In order to learn from experience and continuously improve the transport security system, operators should make post-shipment performance evaluations part of their management process. This process complements information learned during the pre-shipment readiness review and can be incorporated into any future TSPs.

KPIs in the plan should consider both quantitative and qualitative evaluation processes. Such indicators should be evaluated while the transport plan is being tested, as well as during actual transport operations. These evaluations allow timely identification of issues and recommendations for improved performance standards, and they enable the data to be incorporated when upgrading both the design of the transport security system and the TSP. Approaching this process with a spirit of continuous improvement, applying lessons-learned, and regularly seeking more effective, more efficient ways to improve their transport operations is important.

Learning from experience ensures continuous improvement. This includes ensuring physical and technical security enhancements across all modes of transport and transport control centres (TCCs), improvements to response force tactics, weaponry, equipment, and improvements to exercises.
This approach should continue to address new or emerging threats with new technology, revised tactics, changes to techniques and procedures etc. The incorporation of learning from experience, where

applicable, will help ensure transports remain secure and reduces the risk of those involved with them becoming complacent.

Learning from Others

Many other industries also protect their materials whilst in transport, such as bullion, 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.

Helping States and operators who are planning to ship such cargoes for the first time is especially important. This sharing of experience and best practices can be achieved through workshops, tabletop exercises, best practice guides, and coordination or facilitation through nuclear-related organisations such as the IAEA, WINS or WNTI.

There are also a range of industry working groups, the primary one being the WNTI Transport Security Working Group, which provides a platform for operators to come together to discuss and share learning on nuclear material transports. The group also plays an important role in giving the WNTI membership a voice such that consultation on international good practice, guidance and standards are developed for publication. It is also involved in research and development of transport security topics, providing its members with a range of services and support.

06

Suggestions for Further Reading

The Convention on the Physical Protection of Nuclear Material. IAEA Information Circular, INFCIRC/274/Rev.1. Retrieved from www.iaea.org/publications/documents/infcircs/convention-physical-protection-nuclear-material

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.*
NSS. No. 26-G (2015): *Security of Nuclear Material in Transport*

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

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.

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

UN Recommendations on the Transport of Dangerous Goods Model Regulations (the Orange Book)

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 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 www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

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

2.3 Information Security for Operators: Challenges and Opportunities
4.6 Security Exercises

IMO Piracy Reports. Retrieved from: www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Reports/Pages/Default.aspx

IMO International Code for the Safe Carriage of Packaged Irradiated Nuclear Fuel, Plutonium and High Level Radioactive Wastes on Board Ships (INF Code): www.imo.org/en/OurWork/Safety/Cargoes/DangerousGoods/Pages/INF-Code.aspx

World Nuclear Transport Institute (WNTI) – Facts About Nuclear Transport. Retrieved from: www.wnti.co.uk/nuclear-transport-facts/nuclear-transport-facts.aspx

07

Appendix A

Questions to Assess theEeffectiveness 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 organisations 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 Operator (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 competencies your staff possess 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 on 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

Questions for Transport Operators (Carriers)	
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

Questions for the Escort	
Are you confident about 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

08

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 unauthorised interference with the shipment. Relationships with other stakeholders, including regulators and armed response agencies, are excellent. 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 continuous 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. The organisation participates in meetings with other stakeholders. There is a process in place to learn from experience. Individuals engaged in transport operations have been trained. 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. Senior management has limited visibility in transport arrangements. The organisation only participates in meetings with other stakeholders when required. There is no process in place to learn from experience. Individuals engaged in transport operations have limited security training. 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**	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 have not received security training. 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.

World Institute for Nuclear Security

Landstrasser Hauptstrasse 1/18 AT-1030,
Vienna (Austria).
Tel.: +43 1 710 6519
Email: info@wins.org
Web: www.wins.org
International NGO under the
Austrian Law BGBl. Nr. 174/1992
GZ: BMeiA-N9.8.19.12/0017-I.1/2010

ISBN: 978-3-903191-72-3

Whilst the WNTI will use all reasonable efforts to ensure that the information in this Good Practice Guide is accurate, we cannot guarantee the accuracy of all information and we will accept no liability for any loss or damages incurred, howsoever caused, and cannot be held liable for any use or reliance you may make of or put on it. The WNTI also cannot be held liable for your use or inability to use the site or the information or services that it contains. Errors and Omissions Accepted.

The WNTI offers the use of this Good Practice Guide freely to members and non-members of the transport community. Where any interpretation of the information has been made, it has been done so with the interests of the wider transport community. Although the standard has been extensively reviewed by industry experts, if you have any issues in use or content, please contact the WNTI so we can rectify the issues and conflicts in systems etc.

LABS, Victoria House
Bloomsbury Square
London, WC1B 4DA
United Kingdom

Tel: +44 (0)20 7580 1144
Fax: +44 (0)20 7580 5365

Web: www.wnti.co.uk
Email: wnti@wnti.co.uk

WNTI Good Practice Guide
Nuclear Transport Security


wnti