ONR GUIDE			
CLASS A CARRIERS – Transport Security Statements and Plans			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-6.7 Revision 0		
Date Issued:	November 2017	**Review Date:**	March 2020
Approved by:	Dan Hasted	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19076. (2017/419541)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 11/17

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 2).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans, Transport Security Statements (TSS) and Transport Security Plans (TptSP). NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR Inspectors in exercising their regulatory judgment during assessment activities relating to a Class A carrier's TSSs and TptSPs. It aims to provide general advice and guidance to ONR Inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the Class A carrier's arrangements. It does not prescribe the detail, targets or methodologies for Class A carriers to follow in demonstrating they have addressed the SyAPs. It is the Class A carrier's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 NISR defines approved carriers and requires them to have an approved TSS in accordance with Regulation 16 and TptSPs (when required) in accordance with Regulation 19. ONR considers the TSS and TptSP to be important components of a Class A carrier's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 3) and the IAEA Nuclear Security Fundamentals (Reference 4). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle B of the CPPNM refers to the responsibilities of the state during international shipments of NM. Fundamental Principle E describes the security responsibilities of Class A carriers.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 5). Part 6 of that document identifies the requirements for measures

against the theft and sabotage of Nuclear Material (NM) during transport. The Implementing Guide NSS 26G further builds upon the recommendations in NSS 13.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a Class A carrier's TSS and TptSP.

5.2 The HMG Security Policy Framework (SPF) (Reference 6) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that Class A carriers are presented with a coherent set of expectations for the protection of NM in transit, SNI and the employment of appropriate personnel security controls both on and off nuclear premises

5.3 The Classification Policy (Reference 7) indicates those categories of SNI which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 **Objective**. The objective of nuclear transport security is to prevent the theft and/or sabotage of NM in transit outside nuclear premises. Nuclear transport security encompasses all aspects of nuclear security, not just the immediate physical protection of NM being transported outside of nuclear premises.

FSyP 6 – Physical Protection Systems	**Protection of Nuclear Material During Offsite Transportation**	SyDP 6.7
Dutyholders should maintain arrangements to ensure the protection of Category I - III quantities of Nuclear Material against theft and sabotage whilst in transit.		

6.2 **Carrier's Responsibility**. Class A carriers are responsible for the leadership, implementation, operation and maintenance of security arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of NM whilst being transported outside of nuclear premises. Consequently, Class A carriers' security plans should be assessed against the broader framework provided by SyAPs (and associated TAGs) and in accordance with the principles (based upon IAEA guidance) detailed below.

6.3 **Principles of Nuclear Transport Security**. The principles of nuclear transport security are as follows:

- NM 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).

- The number of intermodal transfers should be kept to the minimum.
- No patterns relating to routes or timings should be established.
- NM in transit should not be left unattended.
- Nuclear transportation should be appropriately protected through a graded approach to defence in depth based upon an appropriate design basis threat including appropriate measures to: delay, detect, assess and respond to any malicious activity (including 'insiders') in order to achieve the required Physical Protection Solution (PPS) response and required effect[1].
- All nuclear transportation should be appropriately tracked to enable its location to be known at all times.
- All transport journeys are to be preceded by appropriate security planning and notifications and movements are co-ordinated with relevant agencies and organisations.
- Operational Technology associated with the movement of NM is appropriately protected from compromise.
- Information relating to the movement of NM is appropriately protected and shared on a 'need to know' basis.
- NM in transit is not unnecessarily exposed to known human hazards such as civil disturbances.
- Contingency plans are prepared and practised to ensure that appropriate procedures can be implemented in response to a reasonably foreseeable incident, including unplanned stops.

6.4 **Transport Security Statements**. A TSS should clearly demonstrate that a Class A carrier's nuclear transport security regime is appropriate and facilitates the secure transportation of NM. It should provide sufficient information to demonstrate to an Inspector that nuclear transport security is being applied by the carrier in a proportionate and appropriate manner. A TSS should be:

- **Complete**: The TSS should provide sufficient claims, arguments and evidence that a carrier can achieve the required security outcomes for material in transport. The TSS should not just be a description of a carrier's PPS but should include associated security governance, management and assurance arrangements and the criteria used in nuclear security decision-making.
- **Clear**: The TSS should clearly articulate how all the security functions (and the structures, systems and components that are needed to deliver these security functions) will prevent or mitigate any unauthorised removal or sabotage of NM during transport

[1] See SyAPs Annex D

- **Current**: The TSS should be reviewed, revised and updated to ensure it remains accurate, relevant, and reflects relevant good practice and any lessons identified so that the carrier can continue to achieve the required security outcomes.

Inspectors should consider:

- Whether a carrier has sufficiently strong leadership, robust governance and independent evidence-based assurance processes to support an appropriate nuclear transport security regime.

- Whether a carrier understands their specific legal responsibilities under NISR 2003, including their responsibility to report security incidents and events to ONR.

- Whether a carrier has an organisational culture that appropriately supports nuclear transport security.

- Whether personnel employed in nuclear transport security roles are suitably qualified and experienced (SQEP) for their role.

- Whether the carrier's supply chain management in relation to the procurement of products or services related to nuclear transport security is sufficiently effective.

- Whether the carrier's nuclear transport security regime is sufficiently reliable, resilient and sustainable.

- Whether a carrier's Physical Protection System (PPS), particularly on the conveyances used for the transport of NM, provides appropriate, graded, defence in depth (including access control arrangements for any cargo areas/containers etc.).

- Whether a carrier can protect the confidentiality, integrity and availability of Operational Technology (OT).

- Whether a carrier's Cyber Protection System (CPS) can adequately protect SNI, particularly information relating to the routes, dates, timings and security arrangements relating to the transport of NM.

- Whether a carrier's workforce trustworthiness arrangements can mitigate the threat from an insider, particularly the potential threat from any employees and contractors who are closely involved with the transportation of NM.

- Whether the carrier can facilitate the effective guarding and policing arrangements relating to nuclear transport security, including associated liaison and co-ordination arrangements with the Civil Nuclear Constabulary (CNC), British Transport Police (BTP) and Home Department police/Police Scotland

- Whether a carrier's emergency preparedness and response arrangements are appropriate and well integrated with safety arrangements.

- Whether a carrier's Transport Control Centre (TCC) is appropriately effective and is able to appropriately communicate information and coordinate activity during the movement of NM.

- Whether a carrier's nuclear transport security arrangements are sufficiently responsive to any change in Threat Level.

- Whether the principles of nuclear transport security have been upheld.

6.5 A TSS underpins the ability of a Class A carrier to securely plan, coordinate and conduct the transport of NM; the security arrangements for specific movements of NM are contained within a TptSP.

6.6 **Transport Security Plans**. A TptSP, as required by NISR 2003, is produced in support of a specific movement or series of movements of NM and should reflect how the carrier achieves the required PPS and CPS outcomes through claims, arguments and evidence. A TptSP should adequately address the following areas:

- **Categorisation:** The NM that is to be transported should be accurately categorised for theft and sabotage. The categorisation should inform appropriate security arrangements during its transportation.

- **Compliance**: The TptSP should be submitted to ONR for approval in accordance with the requirements of NISR 2003 (including arrangements for the 7 day notification to ONR).

- **Criteria Used**: The TptSP should provide evidence justifying any criteria used in decision making or option selection relating to the PPS used to protect NM during transport.

- **Completeness:** The TptSP should appropriately describe all security arrangements (both physical and cyber protection systems) for a specific movement of material from when it is handed by the Consignor to the carrier, until responsibility for its security is passed from the carrier to the receiver.

- **Conveyances:** The TptSP should accurately describe the nature of the conveyances being used and how they (and associated containers, compartments and packages) will be searched, sealed, secured, tracked and protected.

- **Confidentiality:** The arrangements to protect SNI and any other sensitive information, including relevant OT systems and information therein, in accordance with the need to know principle, in particular the timings and routes associated with particular movements of NM.

- **Co-ordination and Liaison:** The TptSP should describe the co-ordination and liaison arrangements between the consignor, carrier, consignee and all relevant security/response forces including the CNC, BTP and Home Office police forces/ Police Scotland, irrespective of whether these agencies will issue their own operation orders. Coordination arrangements should include the time, place and procedures for transferring security responsibilities.

- **Command and Control arrangements:** The strategic, tactical and operational command and control arrangements relating to the security of each movement.

- **Communications:** Arrangements for communicating with the transport control centre, the CNC, BTP, Home Office police forces/Police Scotland police and other agencies, including ONR.

- **Contingency Planning:** Arrangements for responding to adversary activities, unplanned stops, safety incidents, environmental conditions, route changes etc., including associated multi-agency training, rehearsals and exercises.

Inspectors should consider:

- In conjunction with ONR SINS and nuclear safety personnel, whether the NM being transported has been accurately categorised and appropriately packaged.

- Whether all relevant security vulnerabilities from both theft and sabotage have been identified and appropriately mitigated.

- Whether the TptSP is supported by authoritative and timely threat assessments.

- Whether all coordinating arrangements have been detailed, particularly who is responsible for security during each phase of the move, how security responsibilities will be transferred between organisations and arrangements for confirming if the movement can proceed.

- If any pattern is being set in relation to the movements of NM (dates, timings, routes) and if so whether it is acceptable.

- Whether the route is as short as possible (consistent with safety/logistic considerations).

- Whether the PPS and CPS, particularly in relation to the conveyances being used, are appropriate.

- Whether the TptSP has undergone an appropriate internal review/quality assurance process within the carrier's organisation.

- Whether appropriate (and SQEP) individuals who have security responsibilities described in the TptSP are specifically named.

- Whether planned route reconnaissance and route searches are appropriate.

- Whether the TptSP is sufficiently responsive to unforeseen delays caused by technical malfunctions of equipment or environmental conditions.

- Whether the TptSP appropriately protects OT and SNI relating to the movement.

- Whether all personnel involved in the move have received appropriate security training and briefings.

- Whether tracking arrangements (and any associated TCC) are appropriate and facilitate the transmission of an emergency call and the subsequent response.

- Whether command, control and communication arrangements are appropriate and sufficiently comprehensive, robust and responsive.

- Whether the size and capability of the guard/response force is appropriate (the relevant CNC operation order should be reviewed in conjunction with the TptSP if the CNC are protecting the movement).

- Whether appropriate training/rehearsals/exercises in support of each movement have been conducted, that they are based on an agreed Design Basis Threat and include all relevant agencies.

- Whether the security arrangements at any planned stops are appropriate.

- Whether contingency planning is realistic and appropriately comprehensive, including arrangements in regard to unplanned stops and the ability to divert a movement onto another suitable route.

- Whether the TptSP has been preceded and supported by appropriate liaison and engagement with all relevant stakeholders.

- Whether lessons identified during previous movements of NM have been incorporated into the TptSP.

- Whether specific security expectations relating to particular modes of transport have been appropriately considered.

- Whether, for international movements of NM, the TptSP has been preceded by appropriate liaison with the relevant authorities of other States and is consistent with written agreements between Her Majesty's Government and other States.

7. REFERENCES

1. **Security Assessment Principles.**
2. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403
3. **Convention on the Physical Protection of Nuclear Material (CPPNM).** https://ola.iaea.org/ola/treaties/documents/FullText.pdf
4. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf
5. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
6. **IAEA Nuclear Security Series No 26G. Security of Nuclear Material in Transport**. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf
7. **NISR 2003 Classification Policy**.

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

8. GLOSSARY AND ABBREVIATIONS

BTP	British Transport Police
CNC	Civil Nuclear Constabulary
CPPNM	Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
NM	Nuclear Material
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
OT	Operational Technology
PPS	Physical Protection System
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
TCC	Tracking Control Centre
TptSP	Transport Security Plan
TSS	Transport Security Statement