



Nuclear Transport Security Guidance for Class B Approved Carriers			
Doc. Type	ONR Guidance Document		
Unique Doc. ID:	CNSS-SEC-GD-001	Issue No.:	1
Record Reference:	2021/23347		
Date Issued:	03/2021	Next Review Date:	03/2024
Process Owner:	P. Fyfe	Deputy Chief Inspector (Civil Nuclear Security and Safeguards)	
Revision Commentary:	New ONR Guidance Document to support approved carriers' efforts to create proportionate and effective transport security statements for approval.		

TABLE OF CONTENTS

1	FOREWARD.....	4
2	THE REGULATION OF NUCLEAR TRANSPORT SECURITY	5
	Introduction	5
	The Objectives of Nuclear Transport Security.....	5
	Principles of Nuclear Transport Security.....	5
	Categories of Nuclear Material	6
	Legal Requirements	6
	Applications for Approval as a Carrier.....	6
	The Approval Process	7
	Notification, Duration and Expiry of Approval.....	8
	Refusal of Applications	8
	The Maintenance of Security	8
	Change of Business Details.....	9
	NISR Directions.....	9
	Reporting of Security Incidents	9
	Revocation of Approval	10
	Appeals	10
3	DETAILED GUIDANCE FOR CLASS B APPROVED CARRIERS	12
	Introduction	12
	TSS	12
	TptSP	12
	Transport Notification	13
	Security Escorts	13
	Foreign flagged vessels.....	13
	Imports of NM.....	14
	Exports of NM.....	14
	Dutyholder Responsibilities	14
	Company security policy.....	15
	Annual Audit or Review of Security Arrangements.....	15
	Workforce Trustworthiness	16
	Cyber Security and Information Assurance.....	16
	Transport Control Centre	17
	Contingency and business continuity planning	17
	Testing and checking of security equipment	18
	Route selection.....	18
	Inspection of load carriers.....	20
	Temporary storage incidental to transport	20
	Intermodal Transfer points.....	20
	Ports and railheads.....	21
	Air Transport.....	21
	Further Security Guidance.....	21

List of Annexes

- A. Format for Transport Security Statements
- B. Transport Security Plans
- C. Notification of the Transport of Category III Nuclear Material from, to or within the United Kingdom
- D. Further Security Guidance (Official-Sensitive:SNI - **Issued separately**)

Abbreviations

Glossary

1 FOREWARD

The Office for Nuclear Regulation (ONR) is the independent regulatory of nuclear safety and civil nuclear security across GB. ONR introduced a new security regulatory framework in March 2017 to facilitate the shift from the prescriptive security regulatory regime to an outcome-focused one. This guidance, the Security Assessment Principles (SyAPs) together with supporting Technical Assessment Guides (TAGs) provides the essential foundation for the introduction of outcome-focused regulation for all constituent security disciplines: physical; personnel; transport; and cyber security and information assurance.

Outcome-focused security regulation supports clarity that responsibility for ownership and control of civil nuclear security rests with dutyholders. The fundamental principles in SyAPs enable the dutyholders to deliver the defined security outcomes, with ONR holding them to account for that delivery. Outcome-focused regulation allows greater flexibility in approach and encourages innovation in security solutions that provide effective and robust protection against the modern threat environment, whilst working in harmony with business processes and maximising opportunities for adding value.

Notwithstanding this flexibility, it is recognised that for those smaller dutyholders, including Class B approved carriers, the effort of developing outcome focused SyAPs-aligned security plans, including transport security statements, needs to be proportionate to the risk. Consequently, this document has been produced to provide a more focused set of guidance to assist those Class B approved carriers to produce a transport security statement which meets regulatory expectations. This approach is designed to facilitate ONR's assessment and approval process and should reduce regulatory burden.

Class B approved carriers that are also licensed sites should employ SyAPs in full in developing transport security statements. Although this document may still be a useful reference for them it does not replace SyAPs and is subordinate to it. The content of this document and Annexes are guidance and should not be seen as prescriptive. Approved carriers always remain responsible for the design, implementation, management and maintenance of security arrangements.



Paul Fyfe
Deputy Chief Inspector (Civil Nuclear Security and Safeguards)

2 THE REGULATION OF NUCLEAR TRANSPORT SECURITY

Introduction

2.1 This Guidance is issued by the Office for Nuclear Regulation (ONR) to support approved carriers' efforts to create proportionate and effective transport security statements for approval. It thereby supports implementation of those parts of the Nuclear Industries Security Regulations (NISR) 2003 that relate to the secure offsite transportation of Category III nuclear material (as defined in the Schedule to the Regulations)¹.

2.2 This document indicates how the requirements of Part 3 of NISR can be satisfied, including those relating to the approval of carriers by ONR. These requirements apply equally to operators of nuclear premises who undertake the transport of nuclear material outside their nuclear premises and also to non-UK carriers who transport Category III nuclear material in the UK. The Regulations do not apply to any transport of nuclear material for the purposes of the Secretary of State for Defence, the transport of Other Radioactive Material, or the transport of Category IV nuclear material outside nuclear premises. Those engaged in transporting Category III nuclear material outside nuclear premises require prior approval as a Class B carrier unless they are already approved as a Class A carrier.

The Objectives of Nuclear Transport Security

2.3 The objective of nuclear transport security is to prevent the theft or sabotage of nuclear material while in transit outside nuclear premises.

Principles of Nuclear Transport Security

2.4 The principles of Nuclear Transport Security are as follows:

- Nuclear material should only be transported outside 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 a minimum.
- No patterns relating to routes or timings should be established.
- Nuclear transportation should be appropriately protected using a graded approach and defence in depth including appropriate measures to: deter, detect, delay and deny malicious activity, including the potential threat from 'insiders'.
- Arrangements should always enable the location of all nuclear transports to be known.
- All transport journeys are preceded by appropriate security planning and notifications and movements are appropriately co-ordinated with relevant agencies and organisations.
- Information relating to the movement of nuclear material is appropriately protected and shared on a 'need to know' basis.

¹ The Transport of Category I and II NM is not covered within this guidance

- Nuclear Material 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.
- A nominated individual is to be responsible for nuclear material at each stage during its transportation.

Categories of Nuclear Material

2.5 The quantities of various types of nuclear material to be transported which fall into Category III are defined in the Schedule to the Regulations. These categories apply to all nuclear material regardless of whether that nuclear material is alloyed or otherwise combined with other material of a non-nuclear nature and include nuclear material contained in waste. The total quantity of all nuclear material being transported in a road convoy, on a train, a ship or aircraft is to be aggregated for the purposes of determining the Category of a particular movement (see regulation 3(5) of NISR 2003). Further information is contained in Annex D.

Legal Requirements

2.6 Part 3 of the Regulations sets down security requirements for the carriers of nuclear material, including nuclear material contained in waste. These require a carrier to:

- Obtain prior approval by ONR as a carrier before transporting Category III nuclear material by road, rail, air and by sea through submission of a Transport Security Statement (TSS) setting out the carrier's security systems, procedures and arrangements (Regulations 13-16).
- Ensure preparations for, and the transport of, nuclear material comply with the TSS approved by ONR, subject to any amendment subsequently approved by ONR (Regulation 17).
- Ensure that anyone with access to Category III nuclear material and sensitive nuclear information related to the security of transport holds an appropriate clearance or security clearance (Regulation 17).
- Report specified occurrences to ONR (Regulation 18).
- Notify ONR in writing with relevant details of a transport of Category III nuclear material not less than 7 days before the date on which the transport is intended to commence (Regulation 20).
- Comply with directions made by ONR with respect to the security of nuclear material transport, including any direction not to commence a proposed transport of nuclear material (Regulation 21).

Applications for Approval as a Carrier

2.7 A carrier may only apply for approval if they carry on, or are likely to carry on, the business of transporting civil nuclear material outside a licensed nuclear site or other nuclear premises. It is expected that applications for approval as a carrier will take several months to process, depending on the quality of the TSS that is initially submitted. Therefore, carriers are encouraged to make an application for approval as soon as it becomes apparent that

they may be required to transport nuclear material, as described in the Schedule to the Regulations. Before applying to ONR for approval as a Class B carrier, potential carriers are strongly encouraged to contact ONR to discuss all aspects of the approval system and the regulatory expectations and associated security requirements contained in Annex D.

2.8 The application is to contain the following information on the applicant, their business and their security procedures:

- Where the applicant is a body required by law to be registered by the registrar of companies, the name, registered number and registered office of that body.
- Where the applicant is an association or partnership which is not required by law to be so registered, the full name of each member of the association or each partner in the partnership, and the name of the association or partnership, as the case may be.
- Where the applicant is a sole proprietor, the full name of that proprietor.
- The applicant's trading name, if different from the name given above.
- The telephone number, fax number (if any) and address of the principal office and of all premises from where nuclear material is handled by the applicant.
- The name, telephone number, email address, fax number if any, and address within the United Kingdom of an individual who will act as the main contact point, including for the receipt of any document mentioned in the Regulations from the Secretary of State relating to nuclear material carriage.
- Details of any changes to the applicant's trading activities in the past 5 years should be given.
- The number of staff used by the applicant in the handling and carriage of nuclear material.
- The mode, or modes, of transport for which the applicant is seeking approval, i.e. road, rail, sea and/or air.
- The Categories of nuclear material to be carried.
- A "Transport Security Statement" (TSS) describing the security standards, procedures and arrangements in place for the protection of nuclear material and sensitive nuclear information, including appropriate clearance procedures for those personnel concerned, and arrangements during any temporary cessation of such transport, i.e. during any planned rest stops.

The Approval Process

2.9 ONR will undertake checks to establish that the applicant:

- Is engaged in, or has credible prospects of being engaged in, civil nuclear transport.
- Is suitable to undertake the transport of nuclear material of the type concerned.
- Has in place the appropriate security standards, procedures and arrangements described in their TSS.
- That those of his employees and contractors who will have access to nuclear material and sensitive nuclear information hold an appropriate clearance or security clearance.

2.10 ONR checks may include a visit to the applicant's principal office and/or other relevant locations, including locations where nuclear material may be held during any planned stops. It may also include checks with financial regulators including any records relating to its directors. In the case of foreign carriers, ONR will consult the competent authorities of the country concerned to support assessment of the carrier's suitability.

2.11 ONR will assess the TSS to ensure that it is sufficiently comprehensive. Inadequate areas will be brought to the applicant's attention for remedial action and/or amendment of the TSS. Only when ONR is content that appropriate security standards, procedures and arrangements are in place, and that these are properly described in the TSS, will it approve the application.

2.12 ONR recovers the costs it incurs during regulatory activities, including engagement and assessment described above, in accordance with the Nuclear Industries Security (Fees) Regulations 2005.

Notification, Duration and Expiry of Approval

2.13 Following satisfactory completion of the above process, ONR will notify the applicant in writing that their application is approved and the date of that approval. Unless revoked earlier, approvals are valid for five years. Approved carriers must re-apply to ONR at least 6 weeks before the approval expires to ensure it does not lapse.

Refusal of Applications

2.14 ONR may refuse an application if it does not meet the conditions required. In that event, the applicant will be notified and will have 28 days from the date of ONR's notice to appeal in accordance with the procedure described below.

The Maintenance of Security

2.15 A Class B carrier is legally required to implement the security standards, procedures and arrangements described in their approved TSS. The TSS applies to work during the preparatory and execution stage of a nuclear material transport until responsibility for the security of the material has been handed over to the authorised recipient or, within the UK, another approved Class A or B carrier. This will include ensuring that national security vetting checks have been satisfactorily concluded on all new employees.

2.16 At any stage following approval, a carrier may submit to ONR a proposed amendment to its TSS. If the proposed amendment is considered satisfactory, ONR will notify the carrier in writing. Alternatively, ONR may approve the proposed amendment with such alterations as it may require. In other circumstances, ONR will advise the carrier that the amendment is considered unsatisfactory and the reasons why.

2.17 A carrier may only sub-contract transport of nuclear material to another carrier approved under the Regulations for that type of nuclear material. In that event, the approved sub-contractor becomes responsible for implementing the requirements of the regulations.

Change of Business Details

2.18 An approved carrier is required to inform ONR in writing within 7 days of any change to its telephone or fax number, email or its principal place of business. However, any change to the details of main contact point is to be notified to ONR no later than the time the change occurs.

NISR Directions

2.19 Regulation 21 enables ONR to issue directions to a nuclear carrier, either individually or to all carriers, for the purpose of ensuring the security of nuclear material being transported within or outside UK. Failure to comply with a direction is an offence for which the punishment can carry a fine and/or imprisonment.

2.20 ONR may direct carriers to adopt or implement standards, procedures and arrangements. ONR can also direct an approved carrier not to start a proposed transport; a direction of this nature would normally only be issued if:

- There may be a specific threat to a transport.
- There is uncertainty as to whether the required security arrangements and associated outcomes could be achieved, for any reason.
- A carrier has not submitted a notification or provided all necessary information in a notification of the intended transport.
- If ONR has reason to believe that a carrier would not implement the standards procedures and arrangements described in the TSS.

Reporting of Security Incidents

2.21 Carriers must report the following security incidents to ONR in accordance with Regulation 18:

- Any unauthorised incursion on to, interference with, or other incident threatening the security of any means of conveyance of Category III nuclear material during its transport or any attempted or suspected such incursion or interference.
- Any unauthorised incursion on to premises where Category III nuclear material is being stored incidental to transport or any attempted or suspected such incursion.
- Any incident occurring during the transport of Category I-III nuclear material, or on premises where such material is being stored incidental to transport, involving an explosive or incendiary device or suspected device, or a firearm or replica firearm.
- Any damage to the means of conveyance of Category III nuclear material which might affect the security of that material.
- Any damage to any building or equipment on premises where Category III nuclear material is being stored temporarily during, or incidental to, its transport which might affect the security of that material.
- Any theft, attempted theft, loss or suspected loss or unauthorised movement of, or any interference with, Category III nuclear material during transport.
- Any theft, attempted theft, loss or unauthorised disclosure of sensitive nuclear information or any suspected such theft, loss or disclosure.

- Any unauthorised access to any sensitive nuclear information or any attempt to gain such access.
- Any threat to do any of the above.
- Any failure to comply with the carrier's TSS or any Transport Security Plan (TptSP).
- Any other event or matter which might reasonably be expected to affect the security of Category I-III nuclear material being transported, premises where Category I-III nuclear material is being stored temporarily during the course of or incidental to its transport, or any information falling within regulation 16(2)(c).

2.22 Reports must be made verbally as soon as is practicable and in any case within 24 hours of the incident. A written report is to be made within 48 hours.

2.23 Verbal reports can be made to the ONR Duty Security Inspector via the Civil Nuclear Constabulary's Command and Control Centre (CCC).

Revocation of Approval

2.24 ONR may revoke an approval given to a carrier for any of the following reasons:

- The approved carrier ceases to carry on a business as a carrier of nuclear material.
- The approved carrier fails to comply with the obligations in the Regulations or with a direction given under regulation 21.
- The applicant has supplied false information in his application for approval as an approved carrier.
- ONR is of the view that the interests of ensuring the security of Category III nuclear material require that the approval should be revoked.

2.25 If ONR proposes revoking an approval, it will give the carrier written notice. A carrier then has 28 days from the date of the notice to make representations. Any representation made will be considered before reaching a decision on revoking the approval. ONR will give notice to the nuclear carrier of its decision to revoke the approval and of the reasons for it, or of its decision not to revoke the approval. A carrier may at any time make a written request to ONR for its approval to be revoked.

Appeals

2.26 If ONR proposes not to approve an application or to revoke an approval of an approved carrier, it will write to the applicant or carrier explaining the reasons. The applicant or carrier then has 28 days in which to make representations to ONR. ONR then reaches a decision on the application, taking into account any representations it has received. If ONR will still not approve an application, or withdraw a revocation, it will inform the applicant or carrier in writing, setting out the reasons for its decision. The applicant or carrier then has the right to appeal against that decision. If an appeal is made the decision will be reviewed by a senior official within ONR who was not involved in the original decision-making process. If the applicant or carrier is still dissatisfied by the outcome after this review, they may ask for the matter to be considered by a more senior ONR official, acting on behalf of the Secretary of State for Business, Energy and Industrial Strategy. The official will consider the arguments

and communicate their decision to the Secretary of State. The Secretary of State will notify the applicant of their decision after consulting the Chief Nuclear Inspector.

3 DETAILED GUIDANCE FOR CLASS B APPROVED CARRIERS

Introduction

3.1 This section contains security guidance for Class B approved carriers. Those Class B approved carriers that are based at UK civil licensed nuclear sites should apply the ONR's Security Assessment Principles (SyAPs) - see the ONR website:

<http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf>. This group of carriers, in preparing a TSS, may simply state that the parts of the NSSP that address SyAPs apply equally to transport. Where they do not, and/or where this guidance indicates further transport-specific arrangements are warranted, the TSS should make this clear and address the relevant issues. For other Class B approved carriers, it will be sufficient that the arrangements described in the TSS comply with the guidance contained within the GCBC.

3.2 ONR must be satisfied that a Class B carrier applicant is able to meet the security requirements relating to the transport of Category III nuclear material. A carrier will need to demonstrate that they:

- Have suitable and competent management and staff in place with clearly designated responsibilities for the security of nuclear transports.
- Have appropriate security and risk management policies and procedures.
- Can develop and maintain an appropriate organisational culture that promotes effective security.
- Are able to implement effective workforce trustworthiness measures, including ongoing aftercare arrangements, in accordance with relevant national arrangements.
- Can demonstrate that vehicles, trains, aircraft and ships to be used for transport are equipped with the necessary physical security features and appropriate tracking equipment.
- Have appropriate contingency plans in place and that they are appropriately exercised.
- Can work and communicate effectively and securely with other organisations.
- Can appropriately protect information, including Sensitive Nuclear Information (SNI).
- That they can meet the required Physical Protection System (PPS) and Cyber Protection System (CPS) outcomes and associated responses (See Annex D for further details).

TSS

3.3 Annex A contains an example of the format for a Class B approved carrier's TSS.

TptSP

3.4 TptSPs for the transport of Category III NM are internal company documents prepared by the approved carrier. They should cover that part of the transport for which the carrier is responsible, including the arrangements for collection and delivery to/from a nuclear site or another carrier. The aim of these plans is to ensure that those concerned with the transport of NM put in place and implement appropriate security arrangements for each transport of Category III NM as described in the TSS. These plans may be generic for

transports of similar material between fixed points but are to be specific for all other transports.

3.5 Although TptSPs for Category III NM transports are internal company documents, they may be inspected by ONR. Annex B contains points to be considered when preparing TptSPs. TptSPs for transports of Category III NM must be classified OFFICIAL-SENSITIVE:SN1 and handled accordingly.

Transport Notification

3.6 A Notification of the transport of Category III NM must be sent by the approved carrier to ONR not less than seven days before commencement of the transport. This requirement applies to transports within the UK, worldwide UK flagged vessels, or when an approved carrier has security responsibility for transports to the UK from overseas. Foreign-flagged vessels carrying NM to or from a UK port are also to submit Notifications not less than seven days prior to commencement of a movement. Such Notifications are not required if a vehicle carrying NM is driven on/off the vessel by the driver and that driver stays on the vessel during its voyage. Notifications are to include all of the applicable information (see Annex C) and are to be marked as OFFICIAL-SENSITIVE:SN1 in accordance with NISR 2003 Classification Policy (<http://www.onr.org.uk/documents/classification-policy.pdf>). Except as described below, carriers may assume that unless they hear to the contrary, that the Notification and associated transport security arrangements are acceptable to ONR without any further communication.

3.7 In exceptional circumstances, carriers may be unable to provide the seven days Notification required. In such circumstances the carrier is to seek immediate approval from ONR for the transport, stating what the exceptional circumstances are. This does not remove the legal obligation on each carrier who will still be required to submit a Notification concerning their transport as soon as they are able to do so. **The actual transport of NM is not to be undertaken using these procedures until the carrier has received approval of the Notification from ONR.**

3.8 Changes to details of Notifications, for example change of conveyance, dates or places from or to which the material is to be transported, are also to be in an amended notification submitted at least 24 hours in advance of the movement commencing.

Security Escorts

3.9 ONR may require a transport of Category III nuclear material to be escorted during the whole or part of a journey. Escort arrangements may range from an authorised person accompanying the transport to an escort from the CNC, as deemed appropriate.

Foreign flagged vessels

3.10 In accordance with Regulation 27A of the Regulations, Foreign registered vessels carrying Category III NM entering or leaving a UK port are required to:

- Be flagged to a state party to the Convention on the Physical Protection of NM (CPPNM) and operated in accordance with the provisions of the International Maritime Organisation's International Ship and Port Facility Security (ISPS) Code.

- Comply with the Regulations in respect of submitting a Notification at least seven days in advance of the movement.
- Comply with any ONR Directions.
- Report incidents in accordance with Regulation 18.

Imports of NM

3.11 Imports of NM into the UK, or transiting a UK port, are to be protected in accordance with the Regulations from the point of entry, which is:

- On a foreign flagged vessel, the point at which it enters UK territorial waters. In the case of a foreign flagged Ro/Ro service, the road vehicle onto which the material is loaded must be operated by an approved Class B carrier.
- On a British flagged vessel, the point at which the handover of security responsibility is made at the port of departure, or, in the case of a Ro/Ro service, when the road vehicle onto which the material is loaded (which must be operated by an approved carrier) is driven onto the ferry; or
- Entry into UK airspace for air transport.

3.12 Only approved carriers whose TSS includes provision for air transport can be used to transport Category III Nuclear Material by air.

Exports of NM

3.13 If an approved carrier remains responsible for the security of a consignment being transported in or through another country, then the carrier will be subject to the physical protection requirements of that country. The Regulations apply to exports of NM until:

- If loaded on a foreign flagged vessel subject to paragraph 2.10, the point at which the vessel departs UK territorial waters.
- If loaded on a British flagged vessel, once the ship's Master has handed over security responsibility at the destination port; or
- If being transported by air, the point at which the approved air carrier exits UK airspace.
- Only approved carriers whose TSS includes provision for air transport can be used to transport Category III Nuclear Material by air.

Dutyholder Responsibilities

3.14 Dutyholders are responsible for ensuring that:

- As the consignor, formal advance notification is made to the receiving facility of the date/time and location of delivery; or,
- As the consignee, the consignor is notified of the duty holder's readiness to receive the consignment; and, in either case (as the consignor or the consignee):
 - This information is provided to the carrier/s.
 - Only approved carriers are used for carriage of Category III NM by road, rail and air within the UK and in British registered vessels.
 - If appropriate, licensed packages are used.

- When NM is transhipped through UK airports, this is carried out only by a carrier whose TSS allows for transports by air (see paragraph 3.45).

3.15 Arrangements for the handover of security responsibility must be agreed in writing before each transport, usually in contracts and agreements produced in connection with the transport/series of transports. There must be a clear understanding about the point at which security responsibility is transferred to or from the carrier, and to the consignee or the consignee's agent or carrier. This will not necessarily coincide with the point at which legal ownership of the material or other responsibility is transferred, but will determine which entity has the responsibility for the physical protection of the material, the maintenance of communications, the arrangements for dealing with an incident and the arrangements for recovery if needed. The point of handover of security responsibility is to be clearly defined and unambiguous, e.g. when the container is loaded onto the trailer is not specific enough. A comment such as 'when the crane is disengaged from the container' is more appropriate.

3.16 Planning and execution of individual transports is a management responsibility of the approved carrier. An individual transport is the duration between the points of handover of security responsibility for a consignment of NM from the consignor/previous carrier and the next carrier/consignee. The carrier should consult, as appropriate, with the management and movement officers of consigning and receiving sites and any other carriers or transport agents (shipping or air) concerned.

3.17 The Movement Officer of the consignee site or responsible staff at any intermediate staging or transfer point must report promptly to the Movement Officer of the consignor site if the consignment does not arrive within a reasonable interval after the estimated time of arrival. What constitutes a 'reasonable interval' will depend upon such factors as distance and weather conditions.

Company security policy

3.18 Approved carriers must ensure that all of their staff who are involved at any stage in the transport of NM are fully aware of their responsibilities. In order to meet this requirement, the carrier's TSS is to detail the company security policy, including training and the auditing of security policies and procedures.

3.19 Approved carriers are to be alert to the potential 'insider' threat and reflect this in their company security policy.

3.20 All TSSs or security policies are to include a section describing the manner in which the carrier promotes and maintains a security culture. Refresher security training of those with direct responsibility for the security of NM (drivers and ship's crew, TCC operators and security staff etc.) should be provided at least annually. Records detailing security education and awareness training are to be maintained and made available for ONR inspection.

Annual Audit or Review of Security Arrangements

3.21 Carriers must either audit **or** review their security arrangements against those in their TSS arrangements that they should comply with, at least annually.

3.22 An audit is to verify, in writing, that all standards, procedures and arrangements described within the TSS are being adhered to. The audit should ideally be conducted by someone independent of the processes being audited. Alternatively, a senior manager can review the TSS and confirm, in writing, any findings and recommendations.

Workforce Trustworthiness

3.23 A key aspect in the protection of NM and information relating to nuclear transports is to ensure that unescorted access to NM or knowledge of movement information is restricted to those with a need to have such access, whose trustworthiness has been pre-determined and who are authorised by management. Therefore, any employee or contract personnel who will have unescorted access to Category III NM or information relating to nuclear transports must have the appropriate level of clearance. Unescorted access is defined as that access authorised by company management for a person holding the appropriate level of security clearance and who is not under the direct visual observation of another person whilst in the designated area. Carriers must ensure that all National Security Vetting (NSV) clearances are completed and maintained in accordance with UK national security requirements, SyAPs (where appropriate) and associated documents, and ensure that appropriate aftercare arrangements are in place.

Cyber Security and Information Assurance

3.24 Information, which includes details of the type and quantity of Category III NM and the transport dates, times and routes of a movement, could be procured or intercepted by adversaries and used to plan the theft or sabotage of NM during transport. All transport information is to be distributed on a 'need to know' basis and compartmentalised if appropriate to ensure that persons receive only that information strictly necessary for their particular function and no further in advance than is necessary to enable them to perform that function. Effective information security is a key element in the protection of NM from theft and sabotage; without the assurance of information security at all stages in the planning and execution of NM transport, more rigorous standards of physical protection would be required.

3.25 Some information held or produced by carriers relating to Category III NM is designated as SNI. As such it is required to be protectively marked in accordance with NISR Classification Policy as this information may be of use to any threat source or threat actor in planning malicious acts related to NM. Company TSSs and TptSPs are examples of such information, as is information relating to the time and date of a movement. SNI is defined in the Anti-terrorism, Crime and Security Act 2001 as including:

“information relating to activities carried out on or in relation to nuclear sites or other nuclear premises which appears to the Secretary of State to be information which needs to be protected in the interests of national security”²

3.26. Policy on the classification of information can be found in the NISR Classification Policy. Carriers that store or process SNI information classified OFFICIAL-SENSITIVE are required to comply with the NISR Classification Policy.

² This definition is further amplified in the Regulations as including “information which requires a protective marking in accordance with the classification policy”, this policy being defined as the “NISR Classification Policy” issued by the Secretary of State from time to time.

3.27 Non-UK based carriers are to apply whatever encryption their Competent National Authority deems appropriate to protect SNI that is marked OFFICIAL-SENSITIVE (that is, information that relates to the specifics of a movement of Category III NM).

3.28 Any indication that SNI such as, for example, transport dates, times, routes and nature of the NM in any particular planned transport, has been compromised in advance of a movement is to be reported to ONR immediately in accordance with NISR Regulation 18(5) (g),(h) and (i).

Transport Control Centre

3.29 At all stages and on a regular basis, the position of either the NM container or the load carrier or vessel transporting NM is to be appropriately tracked or monitored by suitable staff within a Transport Control Centre (TCC).

3.30 Regardless of the method chosen for tracking or monitoring TCCs shall meet the following requirements:

- Be operated by an approved carrier from its own premises, or by an organisation with appropriate security arrangements described in the TSS.
- For foreign carriers, be operated by an organisation approved by the relevant competent authority.
- Be staffed by trained and experienced personnel authorised by the TCC's management to have access to nuclear transport information and able to initiate an appropriate response to any incident involving a transport.
- Retain all transport logs for inspection.
- Have immediate access to contingency plans for responses to all reasonably foreseeable occurrences and the ability to co-ordinate a response effectively with the police and other emergency services.

3.31 Any unexplained deviation from the planned route or schedule is to be investigated by the TCC. If the deviation remains unexplained or indicates that there is an increased risk to the transport then contingency plans are to be implemented.

Contingency and business continuity planning

3.32 All carriers of NM are to have contingency plans prepared and exercised. Exercises can be either 'live' or 'desktop' based and should be conducted at least annually. They should test at least one of the contingency plans described within the TSS and should involve all those who might be involved in responding to and managing the incident (particularly vehicle drivers, TCC staff and managers). Records will be held showing the date, a list of those who took part, the scenario, the outcome and any lessons learned/amendments to the TSS/TptSP as a result.

3.33 Carrier's contingency plans are to detail the response to:

- Unauthorised interference with, or attempt to access, NM or a vehicle transporting NM, including, where appropriate, measures to mitigate or minimise the radiological consequences of an act of sabotage during transport.

- Unauthorised incursion on premises where NM is stored or handled incidental to transport.
- Theft or the attempted theft of NM.
- Interference with staff concerned with the transport of NM.
- Theft or attempted theft, or any loss or unauthorised disclosure, of information falling within regulation 16(2)(c) of NISR 2003, or any suspected such theft, loss or disclosure.
- Unauthorised access to any such information or any attempt to gain such access.
- Actual or suspected theft, attempted theft, loss or unauthorised disclosure of SNI.
- Unauthorised access to SNI, or any attempt to gain such access.
- Threats to carry out any of the above.
- Vehicle breakdown, fire, collision, and recovery.
- Sickness or incapacity of the driver/s.
- Delays to a transport that may necessitate a crew changeover.
- Incidents, adverse weather conditions etc which are likely to either impede the progress of the transport or change its planned route at short notice.

3.34 Staff involved in the transport of NM are to be briefed at least annually on the actions to be taken under company contingency plans. Key personnel involved in nuclear transports and the TCC should have check list of actions and contact details in the event of any such incidents. TSSs are to include broad details of these plans, recognising that some details (names, telephone and other contact numbers) are likely to change.

3.35 It is advisable for any company to have in place business continuity plans and management procedures for recovery following the loss or failure of essential business processes or facilities through fire, flood, terrorism or failure of communications or IT systems. These are not required as part of the TSS but ONR may request to examine them. Further detail may be obtained from the Business Continuity Institute on their website: www.thebci.org.

Testing and checking of security equipment

3.36 Prior to any transport the carrier must ensure that all vehicle security equipment is tested to confirm that it is in full working order. Records of these checks will be held by the carrier. Checks are to cover, but are not limited to:

- Tracking devices.
- Immobilisers.
- Alarms.
- CCTV.
- Locks and Keys.
- Communications.

Route selection

3.37 Route selection should seek to minimise the time Category III NM is in transit. Preference should generally be given to selecting the shortest, most direct route with the least number of modal transfers, unless other factors indicate that a longer route is likely to

be more secure. Readily identifiable patterns to transport routes and associated schedules are to be avoided.

Inspection of load carriers

3.38 Load carriers must be inspected before loading NM and after any stop that requires a report to be made to the TCC. Records of these are to be retained by the carrier. The aim of the inspection is to confirm that:

- The load carrier has not been tampered with in any way.
- A suspicious, or unrecognised, device has not been attached or left on the load carrier or to the NM container/s.

Temporary storage incidental to transport

3.39 Normally, the temporary storage of NM is permitted only on licensed nuclear sites. However, there are occasions during transport, e.g. during shipment or intermodal transfer at UK airports or sea ports, when it may be necessary for NM to be stored temporarily in the custody of an air cargo or sea cargo agent or the operator of a sea terminal. ONR does not approve locations; however, the carrier must be satisfied that the arrangements are adequate. In general, the NM will need to be within the Restricted Area (RA) of the port (under the UK Ship and Port Facility (Security) Regulations 2004) or the Restricted Zone (RZ) of the airport (under the Aviation Security Act 1982, as amended by the Aviation and Maritime Security Act 1990).

Intermodal Transfer points

3.40 Intermodal transfer points are those places where NM is held in one mode of transport while awaiting transfer to another mode, where the carrier remains responsible for the security of the consignment. Delivery to and collection from intermodal transfer points should be timed to avoid consignments remaining at such places longer than necessary. A driver or escort accompanying the shipment should remain with, or be near, the vehicle and in the vicinity of the departure point and, where appropriate, in contact with the handling agent.

3.41 In the event of significant delay at the intermodal transfer point the carrier must implement contingency plans to move the consignment to an overnight stopping place or temporary storage or to provide relief for their staff.

3.42 During the actual transfer, representatives of both carriers should be present and must have the means to alert the TCC and the police (if appropriate) in the event of any security incident. ONR does not approve intermodal transfer points; however, the carrier is to satisfy itself that the arrangements are adequate and enable the required PPS outcome.

Ports and railheads

3.43 All transports should be planned to ensure that NM arrives at a port or railhead and is loaded/off-loaded with the minimum of delay. Where, for exceptional reasons NM arrives at a port in advance of planned loading times, vehicles and/or containers should only be left unattended within the RA by the responsible person if:

- The carrier has an assurance from the management of the facility that any interference with or incident concerning the vehicle, or the load, is reported promptly to the carriers' TCC.
- The driver is away from the vehicle for no longer than 30 minutes.

3.44 Where the railhead is owned/operated by an approved carrier, the TSS is to describe the security arrangements relating to the protection of NM.

Air Transport

3.45 Only approved carriers, whereby their TSS includes specific provision for air transport, can be used to transport Category III Nuclear Material by air. Any carrier wishing to carry Category III NM by air must contact ONR for advice at the earliest possible opportunity.

Further Security Guidance

3.46. Further security guidance relating to PPS and CPS outcomes and workforce trustworthiness arrangements are contained in Annex D (OFFICIAL-SENSITIVE: SNI) that is separately available to approved carriers from ONR.

Annex A – Format and Content of Transport Security Statements

The TSS should be a stand-alone document and should fully describe (or reference) the processes that each carrier has:

1. Company Details

- The name, address, telephone number and e-mail details of the senior officer of the company with overall responsibility for the implementation of policy, e.g. the Chief Executive.
- The name, address, telephone, and e-mail details for the security point of contact their nominated deputy and responsible persons at any other site involved in the transport of NM.

2. Company Security Policy

- Information on company practices and management responsibilities for security procedures, including which individual (at Director level) within the company is routinely responsible for security. This can take the form of copies of company security policy statements and security instructions.
- Information on company practices and management responsibilities for security training. This should include an outline of the training to be given to persons with direct responsibility for the security of NM. In particular, security staff should be clear as to their legal responsibilities.
- Arrangements for annual refresher training.
- The audit or review regime implemented by the company to ensure that all policies and procedures within the TSS are being adhered to and that the TSS remains effective.

3. Physical Protection Systems

- Details of load carriers or vessels used: For closed, locked vehicles, details of locks and how keys are controlled during transport and when not in use. For all vehicles details are to include security systems used such as alarms, immobilisers etc.
- Details of arrangements for tracking or monitoring the status and position of the load carrier or vessel including the method and type of tracking equipment and staffing and operation of the TCC.
- Contingency plans for response to incidents while NM is in storage or in transit. This is to detail the reporting arrangements, to whom reports are to be made and what events are covered.
- Arrangements for testing and checking that security equipment is operational and fit for purpose on a regular basis. This is to include the checking/testing of tracking systems, mobile phones, alarms, immobilisers, locks, CCTV and any other equipment, the failure of which may be detrimental to the security of NM in transit.
- The general arrangements for the transport of NM including:

- The selection and scheduling of routes. If a carrier only transports NM on a small number of routes between fixed locations, those routes should be detailed;
 - The inspection of load carriers, prior to loading NM and following a stop.
 - Use of rest stops and overnight stops.
 - The production of TptSPs
 - The production and communication of Notifications
- Handover/takeover of security responsibility. Details of the arrangements and/or procedures for confirming that material has been handed/taken over, including, the determination of nominated individuals and the use of documentation.
 - Where appropriate, details of procedures to ensure security at inter modal points, such as railheads, ports or airports.
 - Security instructions. Who is responsible for preparing security instructions and briefings for staff with direct responsibility for protecting NM and how are these promulgated and revised? Information relating to or a copy of, the security instructions is to be included.
 - Requirements and procedures for the reporting of security incidents during transit. This is to detail how and to whom reports are made and must be in accordance with NISR Regulation 18.
4. Cyber Security & Information Assurance
- SNI concerning Category III nuclear operations is required to be handled, processed, stored, transmitted and disposed of under special precautions. This section should show how the company proposes to achieve the requirements, including the steps to be taken in the event of the loss, theft or unauthorised access to sensitive nuclear information. This can take the form of a copy of the company information security policy.
 - All information relating to movements of NM is to be handled, processed, stored, transmitted and destroyed by the fewest practicable number of people using the 'need-to-know' principle. Details of how this is put into practice are to be included.
5. Workforce Trustworthiness
- Demonstrate how the workforce trustworthiness requirements will be met for security clearance of any personnel under the control of the company who may need unescorted access to NM containers, including drivers, security staff and, where required, appropriate planning and administration staff .
 - Detail how the company ensures that all staff hold the relevant security clearance prior to commencing work involving NM or sensitive nuclear information.
 - Details should also be given of the procedures in place to ensure that persons who have either no clearance or whose security clearance status is unclear do not have unescorted access to NM, information relating to the transport of NM or a loaded vehicle.

Annex B – Transport Security Plans

A TptSP should contain the following information:

- Dates of transport.
- From/to (consignor/consignee/or another carrier)
- Brief details of the route.
- Point of transfer of security responsibility from consignor to consignee or the next carrier;
- Special instructions (including instructions to safeguard keys/locks).
- Contingency plans for responses to incidents involving the transport.
- Details of arrangements for tracking or monitoring the status and position of the load carrier.
- Staffing of the TCC and associated telephone numbers.
- Escort arrangements (if applicable).
- Security arrangements for load compartments.
- Locations of rest stops.
- Security arrangements for rest and overnight stops, temporary storage on route or intermodal transfers.
- How the police and emergency services will be contacted in the event of an incident.

If the approved TSS contains, in full, the details required in any sections below, it can be referenced within the TptSP instead of duplicating the information.

Annex C – Notification of the Transport of Category III Nuclear Material from, to, or within the United Kingdom

To avoid confusion, carriers are asked to supply only the information requested by the template below, (unless specifically requested by ONR).

From: (carrier's name, address and telephone number of responsible person)

To: (designated contact within ONR)

Copy to:

Date:

Movement Serial Number: (this should be a unique serial number comprising the consignor reference together with the carrier's own reference. If any details have changed and a new notification is issued, the unique serial number should be followed by Issue 2/3 etc.)

Date/s of Movement: (departure and arrival)

Locations: (from which and to which the material is being transported)

Consignor: (full address, telephone, name of responsible person)

Previous Carrier (if applicable): (full address, telephone, name of responsible person)

Next Carrier (if applicable): (full address, telephone, name of responsible person)

Consignee: (full address, telephone, name of responsible person)

Route: (broad outline of route/s using road numbers, including planned rest/overnight stops, inter modal transfers, dates and times of transport)

Material and Quantity Carried: (detail all Regulated material transported: fissile content, enrichment, weight and UN number)

Details of the Type and Number of Packages: (only required if the material is to be transported other than in closed, locked vehicle, rail wagon or shipping compartment)

Point of Transfer of Security Responsibility: (location and details of person/organisation authorised to take security responsibility; this will be either the consignee, approved cargo agent or the next mode carrier. In some circumstances, ONR may require copies of documents from consignee or next carrier certifying acceptance of security responsibility)

Additional Information: any specific arrangements relevant to the transport e.g. details of container used to transport NM, storage prior to intermodal transfer (when and where). Location and security arrangements for any overnight stop.

Example of a generic form utilised for notifications with contact details. Please note this form can be used for both ONR CNSS notifications and for ADR notification to the Transport Competent Authority.

Notification of the transport of category III nuclear material from, to or within the United Kingdom

From:	Name	Role	
To:	For the attention of: The Principal Inspector (Transport Security), ONR (CNSS) & ONR Transport Competent Authority		
Email via Egress Switch	ONR-CNSS.Transport@onr.gov.uk & class7@onr.gov.uk		
Fax:	0151 922 7636	Tel:	0203 028 0013
<p>If notification is more than 7 days, using Egress Switch there is no requirement to get agreement prior to sending. If using fax, call ONR to get agreement to send fax notification. Do not send until agreement has been obtained from ONR.</p> <p>If notification is less than 7 days, Egress Switch (as above). If using fax, ring to get agreement to send fax notification, however if there is no reply, it is acceptable to continue with sending fax notification.</p> <p>Refer to the Notes section for advice to follow in urgent or exceptional circumstances (PTO).</p>			
Copy to:		Date:	
Movement Serial Number:			
<input type="text"/>			
Date(s) of Movement	Arrival:	Departure:	
Consignor:			
<input type="text"/>			
Previous Carrier (if applicable):			
<input type="text"/>			
Next Carrier (if applicable):			
<input type="text"/>			

Consignee:		
Package certificate number:		
Material and quantity carried:		
UN number	Total weight	Total enrichment
Contents:		
From:		
To:		
Route:		
Type and number of packages:		
Point of Transfer of Security Responsibility:		
Additional Information:		

Notes

ONR CNSS and ONR Transport are to be notified of all moves of irradiated fuel off site. Exceptionally, short notice moves (Less than 7 days' notice) must be notified to (and approved by) ONR CNSS before they can take place. For short notice moves under 'exceptional' circumstances for operational reasons the following procedure should be followed:

- a) 'Notification of the transport of category III nuclear material from, to or within the United Kingdom' is to be submitted (at least 24 hours in advance of the move) securely by Egress Switch / Fax.
- b) In working hours contact made with the ONR CNSS Transport Security Inspector
- c) If they are not available, contact should be made with the ONR CNSS Transport Security Lead.

Abbreviations

BPSS	Baseline Personnel Security Standard
BTP	British Transport Police
CCC	Command and Control Centre.
CCTV	Closed Circuit Television
CNC	Civil Nuclear Constabulary
CPPNM	Convention on the Physical Protection of NM
CPS	Cyber Protection System
CT	Counter Terrorist
CTC	Counter Terrorist Check
DfT	Department for Transport
FGE	Foundation Grade Encryption
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
NISR 2003	Nuclear Industries Security Regulations 2003
NM	Nuclear Material
NPS	Nuclear Power Station
NRSP	National Railways Security Programme
NSV	National Security Vetting
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PPS	Physical Protection System
RA	Restricted Area
RZ	Restricted Zone
SMEP	Shipboard Marine Emergency Plan
SNI	Sensitive Nuclear Information
SSP	Site Security Plan
SyAPs	Security Assessment Principles
TCC	Transport Control Centre
TptSP	Transport Security Plan
TSS	Transport Security Statement
UKSV	United Kingdom Security Vetting
VOSA	Vehicle and Operator Services Agency

Glossary

access control	Means to ensure that access to assets is authorised and restricted based on business and security requirements.
adversary	Any individual performing or attempting to perform a malicious act. The term threat is used to refer to a postulated adversary against which security measures are designed, whereas an adversary is active and requires an immediate response.
approved carrier	Class a or class b carrier, approved by ONR under the provisions of NIS 2003. A carrier is a person undertaking the transport of category I-III nuclear material and includes both a carrier for hire or reward and a carrier on his own account.
attack	An attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
authorised person	A natural or legal person that has been granted an authorisation. An authorised person is often referred to as a 'licensee' or 'operator'.
clearance	A generic term used to refer to screening of employees that includes both pre-employment checks and national security vetting.
competent authority	A government organisation or institution that has been designated by the state to carry out one or more nuclear security functions.
consignor	Any person, organization or government which prepares a consignment for transport, and is named as consignor in the transport documents.
contingency plan	A part of the security plan or transport security statement (or stand-alone document) that identifies reasonably foreseeable security events, provides initial planning actions, (including alerting appropriate authorities) and assigns responsibilities to appropriate operator personnel and response personnel.
contractor	Company which undertakes work under a contract awarded to it by a civil nuclear company or site licensee. the term includes both main contractor and sub-contractors.
cyber security	The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and

technologies that can be used to protect the cyber environment and organisation and user's assets.

defence in depth

The combination of multiple layers of defence, including both administrative aspects (procedures, instructions, sanctions, access control rules, confidentiality rules) and technical aspects (multiple layers of protection together with measures of detection and delay) that an adversary would have to overcome or circumvent to achieve their objective.

detection

A process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorised act and that is completed with the assessment of the cause of the alarm.

dutyholder

A generic term to describe 'a responsible person', 'approved carriers' and 'relevant personnel' as defined in NISR.

government secure classification

Official-Sensitive, Secret and Top Secret are standard terms used to convey the appropriate levels of protection

required for sensitive nuclear information and assets. Also known as protective markings.

graded approach

The application of physical protection measures proportional to the potential consequences of a malicious act.

guard

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

information security

The preservation of confidentiality, integrity and availability of information.

insider

An individual with authorised access to nuclear facilities or nuclear activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined to have an adverse impact on nuclear security.

intermodal transfer

The transfer of nuclear material between two or more modes of transport (road/rail/air/sea)

international transport

The carriage of a consignment of nuclear material by any means of transportation intended to go beyond the territory of the state where the shipment originates beginning with

the departure from a facility of the consignor in that state and ending with the arrival at the facility of the consignee within the state of ultimate destination.

likelihood	The product of threat and vulnerability.
local police	The term is used to describe any non-CNC police force that has a role to play in the protection of NM/ORM and may include home department police forces, Police Scotland and British Transport Police forces.
movement officer	A radioactive materials transport responsible officer, site movement liaison officer or other manager appointed by a site to be accountable for ensuring the security of nuclear or other radioactive material movements.
need to know	A principle under which user, processes and systems are granted access to only the information, capabilities and assets which are necessary for the execution of their authorised functions.
nuclear material	Nuclear material listed in the table on the categorisation of nuclear material, including the material listed in its footnotes, in section 4 of IAEA nuclear security series no. 13, nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INF/CIRC/225/revision 5).
nuclear premises	A nuclear site on which nuclear material is used or stored and premises within a nuclear licensed site, in which for example, a person who is not the licence holder, i.e. a tenant, uses or stores NM/ORM. a nuclear premise also includes other locations where category i, ii or iii material is used or stored but excludes premises used for temporary storage during approved transportation.
operator	The licensee within the meaning of section 26(1) of the nuclear installations act 1965.
physical protection	Measures (including structural, technical and administrative protective measures) taken to prevent an adversary from achieving an undesirable consequence (such as radiological sabotage, or unauthorised removal of nuclear or other radioactive material in use, storage or transport) and to mitigate or minimise the consequences if the adversary initiates such a malicious act.
radioactive material	Nuclear material, as defined in the CPPNM; radioactive sources, as defined in the code of conduct for the safety and security of radioactive sources and other radioactive substances containing nuclides which undergo spontaneous disintegration (a process accompanied by the

emission of one or more types of ionizing radiation, such as alpha and beta particles, neutrons and gamma rays).

regulatory authority	Any form of institutional control applied to nuclear material or other radioactive material, associated facilities, or associated activities by any competent authority as required by the legislative and regulatory provisions related to safety, security or nuclear materials safeguards.
risk	The potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and associated consequences.
sabotage	Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.
security clearance	The level of clearance for access to NM or ORM or protectively marked official information, assigned to an individual following a graduated system of procedures, conducted by ONR to establish trustworthiness and reliability (vetting).
security control	A method, device or activity designed to provide a degree of protection.
security escort	A person appointed by a movement officer to accompany a consignment for security purposes in accordance with written instructions.
security regime	The security standards, security procedures and security arrangements set out in the approved security plan and applied by the operator for the protection of the site and of any plant, equipment or NM or ORM thereon, or nm in transit.
sensitive nuclear information	Information relating to, or capable of use in connection with, the enrichment of uranium, or information of a description for the time being specified in a notice under section 71 of the energy act 2013.
site	A civil site or establishment in respect of which a nuclear site license has been granted, or other nuclear premises containing Category I, II or III nuclear material.
tenant	Company or its employees who lease premises on a site.
threat	The product of adversary motivation, intent and capability.