ONR GUIDE			
PHYSICAL PROTECTION SYSTEMS			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-6.0 Revision 0		
Date Issued:	January 2018	**Review Date:**	January 2021
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	TRIM Folder 4.4.2.20789. (2017/456612)		
Revision commentary:	Initial Issue		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Nuclear Industries Security Regulations (NISR) 2003 (Reference 9.1) contains requirements for responsible persons to make certain arrangements including standards and procedures to ensure the security of the nuclear premises, Nuclear Material (NM) or Other Radioactive Material (ORM) stored on the premises, Sensitive Nuclear Information (SNI) and standards and procedures for the transportation of Category I - III NM.

1.2 Regulation 4 of NISR requires there to be an approved security plan for each nuclear premises[1] which details those arrangements for the protection of NM/ORM and SNI, including contingency plans. Regulation 7 places the requirement for the dutyholder to maintain arrangements in accordance with the approved plan. Similarly, transporters of Category I-III quantities of NM are required to detail their security arrangements in an approved Transport Security Statement in accordance with Regulation 16 and Regulation 17 requires them to maintain those arrangements. For the purposes of this guide, the term security plan will be used to refer to both approved documents.

1.3 The Office for Nuclear regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 9.7) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

1.4 To assist inspectors, ONR produces a suite of guides to assist them in making regulatory judgements and decisions in relation to the adequacy of compliance. This inspection guide is one of the suite of documents provided by ONR for this purpose.

2 PURPOSE AND SCOPE

2.1 Security plans should be structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guide is to facilitate a consistent and effective approach to inspecting compliance with the arrangements described in the plan and detailed in the underpinning documentation concerning FSyP 6 – Physical Protection System (PPS).

2.2 The judgements made by the inspector will primarily relate to the efficacy of the implementation of arrangements described in evidence that supports the security plan to ensure that associated arguments are fully substantiated. However, ONR takes a sampling approach to regulation and it is possible that elements of evidence within the plan or underpinning the plan were not subject to assessment as part of the approval process. Therefore, when reviewing or inspecting evidence as part of the intervention, the judgement may relate to the adequacy of the arrangements which support the approved plan. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 The guidance should not be regarded as either comprehensive or mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections.

[1] As defined by Regulation 2 of NISR 2003.

2.4 Relevant good practice that can be used to support FSyP 6 inspection activity is available at an international and national level. These include International Atomic Energy Agency (IAEA) Nuclear Security Series documents NSS 20, 13, 7, 8, 9, 11, 25G and 26G. In particular, Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, 'Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)'(Reference 9.2) includes details on the categorisation of nuclear material for theft and recommends that dutyholders prepare a security plan based on a threat assessment or the design basis threat to include sections dealing with design, evaluation, implementation, and maintenance of the PPS. Sections 4, 5 and 6 contain more detailed guidance on the inspection of specific measures that dutyholders should adopt to protect NM/ORM against theft and sabotage. At a national level, the Manual Forced Entry Standard (MFES) developed by the Centre for the Protection of National Infrastructure reflects the independent forced entry testing of physical barriers to classify their performance and approve their use for protecting UK government and national infrastructure. A number of other CPNI documents, available open source and on the CPNI Extranet are also applicable. The ONR document 'Guidance for Class B Approved Carriers' needs to be applied to a small number of Class B carriers (Annex G refers).

3 RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

4 SUMMARY OF FUNDAMENTAL SECURITY PRINCIPLE 6:

4.1 Physical Protection Systems (PPS) integrate people, procedures and equipment for the protection of assets against theft, sabotage or other malicious activity. The design of a PPS requires a methodical approach in which the designer weighs the objectives of the system (i.e. protection of identified targets) and then evaluates the performance of the proposed design to determine how well it meets the objectives.

4.2 The security plan has to demonstrate how the dutyholder delivers the appropriate outcome. The SyDPs are ordered in such a way that starts with a process of target identification for theft and sabotage, followed by a graded model of system design incorporating a security outcome and posture for the system and an assessment of effectiveness through vulnerability analysis.

4.3 The guidance provided is split into seven parts to cover each of the SyDPs that underpin FSyP 6 as follows:

- SyDP 6.1 (**Categorisation for Theft**) - Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorisation for theft. Sites and facilities are categorised according to the quantities and forms of NM and ORM stored or in process, to determine the required outcomes for the PPS.

- SyDP 6.2 (**Categorisation for Sabotage**) - Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorisation for sabotage. Sites and facilities are categorised for sabotage by undertaking a Vital Area Identification (VAI) to determine the required outcomes for the PPS.

- SyDP 6.3 (**Physical Protection System Design**) - Dutyholders should design and implement a PPS that builds defence in depth and meets the required security outcome based on the categorisation for theft and sabotage. In demonstrating how the outcome is achieved, the PPS design should consider how the indicative security postures are matched.

- SyDP 6.4 (**Vulnerability Assessments**) - Dutyholders should satisfy themselves that their PPS achieves the required security outcome through undertaking vulnerability assessments. A structured and systematic vulnerability assessment should validate the efficacy of the PPS using one or more proven methodologies.

- SyDP 6.5 (**Adjacent or Enclave Nuclear Premises**) - Dutyholders should give due consideration to the effects of adjacent or enclave nuclear premises on the maintenance of nuclear security. This will ensure effective arrangements are in place with adjacent nuclear sites or tenants with regard to shared services or contingency/emergency arrangements.

- SyDP 6.6 (**Nuclear Construction Sites**) - Dutyholders should implement a PPS designed to ensure their activities cannot be exploited by an adversary to incorporate a latent defect or vulnerability, or to pose a threat to an adjacent site.

- SyDP 6.7 (**Protection of Nuclear Material during Offsite Transportation**) - Dutyholders should maintain arrangements to ensure the protection of Category I-III quantities of NM against theft and sabotage whilst in transit. The arrangements to demonstrate the outcomes are achieved should be described in the approved Transport Security Statements (TSS) and Transport Security Plans.

5 PURPOSE OF FUNDAMENTAL SECURITY PRINCIPLE 6

5.1 The purpose of FSyP6: The regulatory expectation is that dutyholders will implement and maintain a proportionate PPS that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequences of a successful attack.

5.2 It should be noted that during interventions inspectors will inspect arrangements which provide evidence to underpin arguments and claims set out in approved security plans. The intervention will also include an inspection of the implementation of the arrangements developed by the dutyholder and summarised in the approved security plan. A number of Technical Assessment Guides (TAGs) have been drafted that directly support FSyP6 and should also be taken into account during inspections**.** Additionally**,** a number of other TAGs are also relevant and should be taken into account during inspections (References 9.8 – 9.21).

5.3 Inspectors also need to take account of other relevant technical inspection guides, including TIGs relating to policing and guarding, and emergency preparation and response.

6 GUIDANCE ON ARRANGEMENTS FOR INSPECTING FUNDAMENTAL SECURITY PRINCIPLE 6 – GENERAL CONSIDERATIONS

6.1 There is an expectation that all NM and ORM has been correctly categorised for theft using the appropriate tables in SyAPs Annexes (taking into account the accompanying

notes) and the dutyholder has demonstrated in their security plan how site or facility categorisation for theft has been implemented according to the quantities and forms of all NM and ORM held or used. They should also demonstrate how they identify and manage potential planned or unplanned changes to inventory and/or operations and other security control measures at a site/facility that might affect its categorisation for theft.

6.2 There is an expectation that all NM and ORM has been correctly categorised for sabotage and they have demonstrated in their security plan how site and/or facility categorisation for sabotage has been implemented through the conduct of a VAI study using an agreed methodology. They should also demonstrate how they identify and manage potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorisation for sabotage.

6.3 There is an expectation placed on the dutyholder that they demonstrate in their security plan or associated documentation how the PPS design is capable of meeting the required security outcome, with details of the security posture (Routine, Robust and Fortified) being applied. The postures should be applied adopting a graded approach based on the required security outcome and taking account of the indicative postures defined in the SyAPs Annexes.

6.4 There is an expectation that the dutyholder should demonstrate in their security plan how the effectiveness of the PPS has been validated through the conduct of performance based vulnerability assessments. Such assessments could comprise one or more proven methodologies such as: force-on-force exercises; table top exercises, war gaming, simulation, and computer based modelling or expert analysis.

6.5 There is an expectation that the dutyholder will demonstrate in their security plan how they ensure sharing of information and maintenance of a coherent, coordinated approach towards all aspects of security (and emergency response) that may be influenced by adjacent or enclave nuclear premises.

6.6 There is an expectation that dutyholders demonstrate within their security plan how their PPS is phased according to sensitivity of the site as construction develops in order to provide ongoing assurance that its activities cannot be exploited by an adversary.

6.7 There is an expectation that nuclear transport security will prevent the theft or sabotage of nuclear material in transit outside nuclear premises. Nuclear transport security encompasses all aspects of nuclear security, not just the immediate physical protection of nuclear material being transported outside of nuclear premises.

6.8 There is an expectation that Class A carriers are responsible for the leadership and management, 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 nuclear material whilst being transported outside of nuclear premises.

6.9 There is an expectation that dutyholders demonstrate in the security plan how they ensure that the design and operation of the PPS delivers appropriate levels of redundancy, diversity, segregation and resilience.

6.10 There is an expectation that these arrangements are underpinned by strong leadership, robust governance and management arrangements, and incorporate effective processes to deliver evidence-based assurance.

6.11 There is an expectation that the arrangements are underpinned by effective and timely stakeholder engagements that ensure that the operational effect and PPS outcomes are delivered in an integrated manner.

6.12 There is an expectation that arrangements are supported by comprehensive change management processes that ensure that all stakeholder's individual plans and responsibilities are aligned at all times, and that amendments are recorded and version controls implemented.

6.13 There is an expectation that arrangements are reviewed on changes to the threat, security posture, hazard profile or any other occasion that warrants consideration and that would fundamentally impact upon the PPS or response outcome. Regardless of the need to review on significant change, it would also be expected that arrangements are routinely reviewed to ensure that they remain valid and that no omissions or inaccuracies exist.

6.14 There is an expectation that the Systems and Structures that are necessary to deliver these arrangements are supported by Examination, Inspection, Maintenance and Testing (EIMT) processes and procedures and appropriate evidence retained for assurance purposes.

6.15 There is an expectation that the security plan will identify the nature and intervals of EIMT for key elements of the security system and provides appropriate justification for any long term performance claims based on the approach to EIMT. EIMT activities should take account of any reliability claims in the security plan and be appropriate for the life cycle and/or PPS outcome required of the site.

6.16 There is an expectation that the security plan will identify how the dutyholders' arrangements ensure sustainability of the nuclear security regime at their site and/or facilities.

6.17 There is an expectation that dutyholders will describe in the security plan how they seek assurance of supplier capability to support effective nuclear supply chain management arrangements.

6.18 Inspectors should also consider a range of generic topics such as 'change management'.

7 GUIDANCE ON INSPECTION OF FUNDAMENTAL SECURITY PRINCIPLE 6 ARRANGEMENTS AND THEIR IMPLEMENTATION

7.1 **Preparation** – As part of the preparation phase it may be appropriate for the inspector to obtain evidence in advance to consider in detail prior to arrival at site. This consideration in advance may influence the focus and delivery of the intervention. It is recommended that the requirements during the delivery phase are clearly identified to the dutyholder in good time for them to prepare effectively. This may include documents relating to EIMT schedules, and/or change control or change modifications. The inspector should also make them aware of the staff and stakeholders that they need to see as part of the intervention. This might include representatives from the Civil Nuclear Constabulary (CNC), Contract Guard Force, project management, security engineering and nuclear material accountancy.

7.2 **Planning** – The inspector should be clear as to the purpose of the proposed intervention and why is it being considered; is it regulatory intelligence, divisional strategy, routine compliance or another reason that is driving the requirement? Once these initial considerations are understood the inspector should be in a position to

define and agree the outcomes and outputs of the intervention. Once the outcomes and outputs of the intervention are defined the inspector will be in a position to identify the inputs required to deliver outputs; this is likely to be ONR resource and support may be required from outside of the division. For further guidance see HOW2 – Planning and Conducting Interventions.

7.3 **Delivery** – The inspector should adopt a proportionate and graded approach utilising the history from previous interventions to inform their expectations. They should ensure that any issues identified in previous interventions have been followed up. The inspector should apply the principles of inspection found in ONR- INSP-GD-064.

7.4 Specific considerations related to the arrangements for each of the FSyP 6 elements are covered in the Annexes as follows:

- **Annex A** - SyDP 6.1 (Categorisation for Theft)
- **Annex B** – SyDP 6.2 (Categorisation for Sabotage)
- **Annex C** – SyDP 6.3 (Physical Protection System Design)
- **Annex D** – SyDP 6.4 (Vulnerability Assessments)
- **Annex E** – SyDP 6.5 (Adjacent or Enclave Nuclear Premises)
- **Annex F** – SyDP 6.6 (Nuclear Construction Sites)
- **Annex G** – SyDP 6.7 (Protection of Nuclear Material during Offsite Transportation)

8 FURTHER READING

8.1 Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403

8.2 IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011.

8.3 IAEA Nuclear Security Series No. 20. Objective and Essential Elements of a State's Nuclear Security Regime.

8.4 Convention on the Physical Protection of Nuclear Material (CPPNM)

8.5 HMG Security Policy Framework. Cabinet Office.

8.6 NISR 2003 Classification Policy.

8.7 Security Assessment Principles.

8.8 Nuclear Transport Security - Guidance for Class B Approved Carriers

8.9 CNS-TAST-GD-6.1: Target Identification for Theft.

8.10 CNS-TAST-GD-6.2: Target Identification for Sabotage.

8.11 CNS-TAST-GD-6.3: Physical Protection System Design.

8.12 CNS-TAST-GD-6.4: Vulnerability Assessment.

8.13 CNS-TAST-GD-6.5: Adjacent or Enclave Nuclear Premises.

8.14 CNS-TAST-GD-6.6: Nuclear Construction Sites.

8.15 CNS-TAST-GD-6.7: Class A Carriers Transport Security Statements and Plans.

8.16 CNS-TAST-GD-3.3 – Measurement of Competence.

8.17 CNS-TAST-GD-4.4 – Commissioning.

8.18 CNS-TAST-GD-5.1 – Reliability and Resilience.

8.19 CNS-TAST-GD-5.2 – Examination, Inspection, Maintenance and Testing.

8.20 CNS-TAST-GD-5.3 – Sustainability.

8.21 CNS-TAST-GD-7.3 – Protection of Nuclear Technology and Operations.

Annex A - SyDP 6.1 (Categorisation for Theft)

Standards and Expectations

There is an expectation that all NM and ORM has been correctly categorised for theft using the appropriate tables in SyAPs (taking into account the accompanying notes). The dutyholder should demonstrate in their security plan how site or facility categorisation for theft has taken account of the quantities and forms of all NM and ORM, including radioactive sources, held or used. They should also demonstrate how they identify and manage potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorisation for theft. There should be a clear interface between the facility and Nuclear Material Accountancy and Control (NMAC) system.

Inspectors should consider:

- Are accountancy records held by NMAC for individual facilities and do they accord with the categorisation declared in the security plan?
- Have the total quantities of material been aggregated to ensure the correct categorisation has been recorded?
- Is there accurate, timely, complete and reliable information on the locations, quantities and characteristics of NM in the facility?
- Are characteristics of NM kept under review if the form of the material has a significant role in its categorisation?
- Do source stores detail inventories and source categorisations and accord with the categorisation declared in the security plan and or source register?
- Is there a process in place to identify and manage potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorisation?
- Is there an appropriate review process which is initiated by either periodicity or change management?
- Do NMAC arrangements cater for NM to be acquired in a single event of theft or acquired in small amounts during several protracted theft events?
- Is appropriate security training provided for NMAC personnel?
- Is there is a strong working relationship between NMAC and the facility personnel?
- Do all facility personnel have a clear understanding of the importance of NMAC to security?

Annex B – SyDP 6.2 (Categorisation for Sabotage)

Standards and Expectations

There is an expectation that sites and facilities have been correctly categorised for sabotage. The dutyholder should demonstrate in their security plan how the site and/or facility categorisation for sabotage has been implemented through the conduct of a VAI study using an appropriate methodology. Dutyholders should also demonstrate how they identify and manage potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorisation for sabotage

Inspectors should consider:

- Are personnel employed to carry out VAI suitably qualified and experienced (SQEP)?
- Is there an effective interface between operational/safety personnel and security personnel in carrying out the VAI?
- Do the inventories and processes in facilities match that detailed in VAI reports?
- Are processes in place to identify potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its sabotage categorisation and trigger a review of the VAI?
- Is there a process in place to identify changes in the NIMCA or in passive physical security protection barriers that underpin the VAI study and are these kept under review and the VAI re-applied if significant changes are identified?

Annex C – SyDP 6.3 (Physical Protection System Design)

Standards and Expectations

An effective PPS design comprises of people, procedures and equipment working in combination to achieve a desired outcome and this should be considered and taken into account during inspection activity. The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how the PPS design is capable of meeting and implementing the required security outcome and it is clearly evidenced and demonstrated or referenced in the plans. There is also an expectation that dutyholders will maintain records of any performance based testing. Consequently, the security plan and supporting evidence such as the results of any performance based testing will be the start point for inspection activity. When assessing the reliability, resilience and sustainability of security structures, systems and components, the relevant ONR TIG should be taken into account including CNS-INSP-GD-005.

Inspectors should consider:

- Are personnel employed in PPS design roles as detailed in the security plan or associated documents suitably qualified and experienced (SQEP)?
- Are those employed in security roles appropriately SQEP to perform their function?
- Is supply chain management in relation to the procurement of products or services related to nuclear security sufficiently effective?
- Are appropriate controls and procedures in place to ensure the security system design delivers the functional requirements and meets the relevant standard(s)?
- Is a structured process used to identify and define security requirements for example, the operational requirements process, and has the reliability, resilience and sustainability of the required security system and its components been specified?
- Are the structures, systems and components and people and processes that deliver key security functions supporting the posture claimed in the security plan, clearly described, designed, implemented and maintained according to their importance?
- Are operational procedures in place which defines action to take in the event of a system, structure or component failure? Do they include guidance on substitution options? Are the procedures periodically reviewed and updated?
- Are dependencies identified during any vulnerability assessment activity fully operative and subject to effective EIMT arrangements?
- Has the insider threat been adequately mitigated? Do the operational procedures for the dependencies and supporting systems define their importance and the associated implementation of maintenance activities?
- Are security arrangements sufficiently responsive and scalable to any change in threat level or a change in a specific threat?
- Are command, control and communication arrangements relevant to the PPS clearly defined, appropriate and sufficiently comprehensive, robust and responsive?

- Is contingency planning in relation to the PPS effective, realistic and appropriately comprehensive?

- If a PPS is a Computer Based PPS (CB-PPS), has SyDP 7.3 for Operational Technology (CNS-TAST-GD-7.3) been taken in to consideration?

- Has consideration been given to the implementation of a two man rule to mitigate the insider threat, where appropriate**?**

- Has the dutyholder justified their solutions by the use of relevant good practice, such as:
  - CPNI – Hostile Vehicle Mitigation Guide, including the use of Vehicle Dynamics Assessments etc.
  - CPNI - Manual Forced Entry Attack Standard (MFES)
  - CPNI – Security Lighting – Guidance for Security Managers

Annex D – SyDP 6.4 (Vulnerability Assessments)

Standards and Expectations

There is an expectation that the dutyholder should demonstrate in their security plan how the effectiveness of the PPS has been validated through the conduct of structured and systematic vulnerability assessments. Such assessments could comprise one or more proven methodologies such as: force-on-force exercises; table top exercises, war gaming, simulation, and computer based modelling or expert analysis. When reviewing vulnerability assessments, inspectors may enhance their knowledge and understanding by undertaking a visual inspection by 'walking the ground' in addition to scrutinising documentation and any dutyholder presentations.

Inspectors should consider:

- Is the extant vulnerability assessment/performance based testing carried out in support of security plan approval valid noting that MFES ratings change as forcible attack equipment improves?
- Is there a procedure/process for revalidating vulnerability assessments as required to take into account any changes to the threat, risk or security posture?
- Are any vulnerability assessments carried out based on all relevant malicious capabilities described in the NIMCA document?
- Review the vulnerability assessment with the dutyholder to confirm they have appropriately identified and considered all adversarial path analysis and utilised accurate detection and delay times and that these remain extant.
- Have the extant MFES ratings been applied to vulnerability assessments?
- Review the vulnerability assessment with the dutyholder to confirm that the scenario analysis remains credible, challenging, transparent and considers the possibility of sub-optimal performance by the response force.
- If the PPS is required to achieve Outcome 1 or 2[2], how has the dutyholder confirmed that the vulnerability assessment interruption analysis remains appropriate?
- If the PPS is required to achieve Outcome 1, is the vulnerability assessment neutralisation analysis appropriate?
- Where appropriate have CNC or guard force response times to meet PPS outcomes been validated and are they kept under review?
- Review the vulnerability assessment with the dutyholder to confirm that it records all potential vulnerabilities in the PPS and any associated risks of not delivering the defined posture or outcome.

[2] Outcome tables from Annex C and Annex H of the OFFICIAL SENSITIVE SyAPs Annex

Annex E – SyDP 6.5 (Adjacent or Enclave Nuclear Premises)

Standards and Expectations

Inspection and assessment by ONR inspectors should focus on ensuring that individual dutyholders take responsibility for ensuring all the elements of their security regime, whether they are provided by a contractor or an adjacent or enclave site, integrate effectively. This will be reflected in the security plans in order to ensure there are clear lines of accountability and the claimed effects of the PPS are met for all relevant dutyholders.

Dutyholder security plans should clearly articulate the shared services provided by or for the benefit of the adjacent or enclave site and the impact that one may have on the other. This includes shared contingency/emergency arrangements.

Emergency response arrangements for a dutyholder site that has adjacent or enclave premises must take into account the risks and hazards presented by all dutyholders and deliver an appropriate means of emergency communications across them to ensure the planned response is effective. Regular dialogue and joint training and exercising amongst dutyholders are needed to ensure a consistent and coherent emergency response.

Inspection and assessment by ONR inspectors should seek to identify that clear lines of communications between dutyholders exist, and there are identified and established points of contact for all matters pertaining to security and emergency response. It is considered good practice for dutyholders to have regular formal meetings with agreed terms of reference to consider and review security and emergency response protocols amongst adjacent or enclave sites.

Where the adjacent or enclave nuclear premises is undergoing modification, the dutyholder should be fully aware of project timelines and take into account the changing risks and hazards as an adjacent project develops. This is equally true for adjacent sites undergoing decommissioning, where certain security systems may no longer be supported once nuclear inventory is removed and the categorisation for theft and sabotage reduced.

Inspectors should consider:

- Are there arrangements in place to ensure that a coherent, integrated and coordinated approach has been taken to all aspects of security that may be affected or influenced by any adjacent or enclave nuclear premises?
- Are all shared services and responsibilities for their delivery detailed in the plan effectively implemented?
- Do the emergency arrangements take into account the risks and hazards presented by all adjacent and enclave nuclear premises?
- Is there regular dialogue, joint training and exercising to ensure a coherent emergency response between adjacent and enclave nuclear premises?
- Is there an appropriate level of liaison and information exchange to ensure a shared understanding of current security plans and any planned changes to site categorisation or security arrangements?

Annex F – SyDP 6.6 (Nuclear Construction Sites)

Standards and Expectations

Construction sites can present unique challenges to security taking into account factors such as development from open sites, potential workforce of several thousands and their proximity to existing nuclear facilities. There is an expectation that dutyholders demonstrate within their security plan how their PPS is phased according to sensitivity of the site as construction develops in order to provide ongoing assurance that its activities cannot be exploited by an adversary. The inspector should ensure that, as the site develops and nuclear material is introduced, the appropriate security outcome has been correctly identified and met, and inspections also take cognisance of the standards and expectations laid out in Annexes A – D of this TIG.

Inspectors should consider:

- Has a company security manager and a member of the senior management team been appointed to oversee the delivery of security?
- Has a Site Security Manager or SQEP senior manager been appointed to act as the security focal point for liaison with the adjacent site and to oversee security force activity?
- Does the Construction Site Manager/Director have a clear understanding of the risks to the construction site and adjacent site and have clear responsibilities for security governance?
- Is there effective liaison and information exchange arrangements in place with any adjacent nuclear premises?
- Have hazards associated with construction activity been identified and mitigated and kept under regular review?
- Has the NIMCA been used as a basis for an evaluation of the vulnerabilities and hazards to ensure appropriate security arrangements are in place to mitigate the associated risks of construction projects?
- Are access control arrangements effective? Do they incorporate security control points, expect searching and make provision for the use of secure compounds in accordance with the plan?
- Is there adequate control of the supply chain?
- Are effective arrangements in place with primary and sub-contractors including establishment of contractor security liaison managers, regular meetings, security clauses in contracts?
- Is there a clear and effective personnel security strategy?
- Is there an effective strategy in place to foster a strong security culture amongst staff and contractors?
- Is there an appropriate site boundary in place that allows enforcement of the Serious Organised Crime and Police Act 2005 once the nuclear site licence is granted?

- Have appropriate operational controls been implemented to manage risks to adjacent sites, such as key control?
- Have incremental measures been tested and confirmed as effective in advance of increases in security risk (i.e. categorisation for theft, sabotage or classification of SNI)?
- Does the plan define arrangements to manage the risk of defects and malicious damage? Are they implemented?

Annex G – SyDP 6.7 (Protection of Nuclear Material during Offsite Transportation)

Standards and Expectations

There is an expectation that nuclear transport security will prevent the theft or sabotage of nuclear material in transit outside nuclear premises. Nuclear transport security encompasses all aspects of nuclear security, not just the immediate physical protection of nuclear material being transported outside of nuclear premises (see Class B Carriers below).

Inspectors should consider:

- Are the governance and independent evidence-based assurance processes detailed in the Transport Security Statement implemented effectively?
- Are personnel employed in nuclear transport security roles suitably qualified and experienced (SQEP) for their role?
- Is the carrier's supply chain management in relation to the procurement of products or services related to nuclear transport security effective?
- Is the carrier's nuclear transport security regime reliable, resilient and sustainable?
- Are the carrier's emergency preparedness and response arrangements appropriate and well integrated with safety arrangements and implemented in accordance with the approved TSS?
- Does the PPS applied to nuclear transport security adopt a graded approach and provide appropriate defence in depth?
- Have the appropriate 'PPS Outcomes and Required Effect' and 'PPS Response and Required Effect' for the category of nuclear material being transported been identified and achieved?
- Are arrangements in any evidence selected as part of the intervention (TSS or associated documentation) effectively implemented and fully support arguments and claims?
- Is the carrier's Transport Control Centre (TCC) able to appropriately communicate information and coordinate activity during the movement of NM and compliant with the TSS?
- Are the PPS and Cyber Protection System, particularly in relation to the conveyances being used, appropriate?
- Are command, control and communication arrangements appropriate and sufficiently comprehensive, robust and responsive?

Class B Carriers

SyAPs applies to all approved carriers but ONR takes a proportionate approach to its application in relation to the size and structure of carrier organisations, which varies from large multi-national companies and site licensed companies to smaller road haulage operations.

Therefore, for smaller carriers ONR has produced the Guidance for Class B approved carriers (Reference 9.8). Those Class B approved carriers that are based at UK civil licensed nuclear sites will apply SyAPs in its entirety (where applicable). This group of carriers, in preparing a TSS, may simply state that the parts of the security plan that address SyAPs apply equally to transport. Where they do not, and/or where the Class B 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 in the ‘Guidance for Class B Approved Carriers’.