



OFFICIAL

1

ONR GUIDE			
NUCLEAR CONSTRUCTION SITES			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-6.6 Revision 1		
Date Issued:	March 2020	Review Date:	March 2023
Approved by:	Brett Roberts-Howe	Professional Lead	
Record Reference:	CM9 Folder 4.4.2.24831. (2020/100302)		
Revision commentary:	First Revision issued		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP TO RELEVANT LEGISLATION.....	2
4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE	2
5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS	3
6. DEFINITION OF A NUCLEAR CONSTRUCTION SITE	4
7. ADVICE TO INSPECTORS	4
8. NUCLEAR CONSTRUCTION SITES – GENERAL	5
9. SECURITY ARRANGEMENTS FOR A NUCLEAR CONSTRUCTION SITE	7
10. CLICENCED NUCLEAR SITE UNDER CONSTRUCTION	10
11. MULTIPLE UNIT SITES.....	ERROR! BOOKMARK NOT DEFINED.
12. REFERENCES	13
13. GLOSSARY AND ABBREVIATIONS	14
APPENDIX 1 – SUMMARY OF INDICATIVE MEASURES FOR NUCLEAR CONSTRUCTION SITES.....	15
APPENDIX 2 – SUMMARY OF INDICATIVE MEASURES FOR CIVIL LICENCED NUCLEAR SITES UNDER CONSTRUCTION SITES	17

OFFICIAL

OFFICIAL

1. INTRODUCTION

- 1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 2).
- 1.2 The term ‘Security Plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

- 2.1 This TAG contains guidance to advise and inform ONR inspectors in the exercise of their regulatory judgement during intervention activities relating to assessment of physical¹ protection at nuclear construction sites. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

- 3.1 The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licenced 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.
- 3.2 NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved Security Plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers Physical Protection Systems (PPS) to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

- 4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 3) and

¹ For the purposes of this TAG, physical protection also refers to Cyber Security & Information Assurance and Personnel Security arrangements.

OFFICIAL

OFFICIAL

the IAEA Nuclear Security Fundamentals (Reference 4). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

- 4.2 Fundamental Principle C of the CPPNM refers to the legislative and regulatory framework which should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorisation. The importance of issues relating to authorisation is reiterated in the Nuclear Security Fundamentals, specifically:
- Essential Element 3: Legislative and Regulatory Framework – 3.3 The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime provides for the establishment of nuclear security regulations and requirements, and associated procedures for evaluating applications and granting authorisations or licences.
- 4.3 A more detailed description of issues relating to legislative and regulatory frameworks is provided in Recommendations level guidance, specifically paragraphs 3.8 to 3.17 of Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 5). This document recommends that the State should licence activities or grant authorisation only when such activities comply with its physical protection regulations.
- 4.4 The IAEA also publish Implementing Guide NSS No. 19 'Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme' (Reference 6) where further relevant information can be found on legislative and regulatory frameworks at paragraphs 3.1 to 3.12.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

- 5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 6.6 – Nuclear Construction Sites, in support of FSyP 6 – Physical Protection Systems. The TAG is consistent with other TAGs and associated guidance and policy documentation.
- 5.2 The HMG Security Policy Framework (SPF) (Reference 7) describes the Cabinet Secretary's expectations of how HMG organisations, and third parties handling HMG information and other assets, will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.
- 5.3 The NISR 2003 Classification Policy for the Civil Nuclear Industry (Reference 8) indicates those categories of SNI, which require protection and the level of security classification to be applied.

OFFICIAL

OFFICIAL

6. DEFINITION OF A NUCLEAR CONSTRUCTION SITE

- 6.1 Section 77 of the Anti-Terrorism, Crime and Security Act 2001 (Reference 9), defines the term 'Nuclear Construction Site' as a site on which works are being carried out with a view to it becoming a nuclear site wholly or mainly for purposes other than defence purposes, which is situated within 5 kilometres of an existing nuclear site. NISR 2003 further defines a 'Nuclear Construction Site' as one which works are being carried out by a developer pursuant to the grant or issue of a planning or development consent order.

7. ADVICE TO INSPECTORS

- 7.1 Nuclear construction sites present unique challenges to security, not least the scale of some projects, extent of activity and numbers of personnel involved. All SyAPs and their associated TAGs will be relevant to nuclear construction site security at some stage and this TAG does not intend to reproduce the content of those TAGs. The aim of this TAG is to highlight to inspectors the differences a construction site has to an operational site to allow for proportionate assessment. It is a key principle that security measures are effective and proportionate to the risk, and inspectors should recognise that dutyholders need flexibility to manage changes to the construction process. The threat will change as the project progresses. During the earlier stages (prior to NM on site), the main threat from a regulatory perspective, will be the threat to the adjacent site (if within 5km) and the malicious introduction of defects. Both of these may involve the 'insider' threat. Once NM is on site, the full spectrum of threat actors as described in the UK Design Basis Threat (DBT) will apply. Inspectors should be open to innovative proposals whilst ensuring risks are appropriately mitigated.
- 7.2 In addition to the SyAPs FSyPs, throughout the duration of the project, the developer / dutyholder should demonstrate complete cognisance of the SyAPs Key Security Plan Principles (KSyPPs), such as the threat, the graded approach and defence in depth. These KSyPPs are applicable during all phases and provide the necessary framework for the continuous evolution of the protective security regime.
- 7.3 The following list of TAGs whilst not exhaustive, are particularly relevant to this TAG:
- Guidance on the Security Assessment of Generic New Nuclear Reactor Designs
 - Governance and Leadership
 - Capable Organisation
 - Maintenance of a Robust Security Culture
 - Oversight of Suppliers of Items of Services of Nuclear Security
 - Adjacent and Enclave Sites
 - Categorisation for Theft
 - Categorisation for Sabotage
 - Physical Protection Design
 - Commissioning of Security Systems
 - Guidance on the Purpose, Scope and Quality of a Nuclear Site Security Plan

OFFICIAL

OFFICIAL

- 7.4 The purpose of the assessment is to determine whether the security arrangements on a Nuclear Construction Site are adequate to address three specific risks:
- The threat a Construction Site may pose to a neighbouring nuclear site (within 5km)
 - The risk of sabotage through introducing defects into the new nuclear facility while it is under construction that could compromise the safety or security of the nuclear facility once it starts operations
- 7.5 The assessment should also provide a level of confidence that the facility is being constructed to meet the arrangements that will be detailed in the Security Plan once the facility becomes operational applying the SyAPs KSyPPs, including 'secure by design', the graded approach, defence in depth, the threat etc.

Regulatory Expectation

- 7.6 The regulatory expectation is that dutyholders demonstrate within their Security Plan how their physical protection system 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.

FSyP 6 – Physical Protection System	Nuclear Construction Sites	SyDP 6.6
Dutyholders should ensure that they implement a physical protection system ² designed to ensure its activities cannot be exploited by an adversary to incorporate a latent defect or to pose a threat to an adjacent site.		

8. NUCLEAR CONSTRUCTION SITES – GENERAL**Phased Approach**

- 8.1 In order to provide for effective and proportionate security arrangements throughout the lifetime of the construction project, it is important that a phased approach is adopted. The phases should identify key points during the construction process when it is necessary to make incremental security enhancements to reflect the rise in the level of risk as the project progresses. Each phase should be documented in the Construction Site Security Plan (CSSP), and subsequently in the post-licensing Security Plan, together with the associated security arrangements clearly articulated for each phase. Security 'hold points' should be identified before progressing from one phase to the next to provide time to assess and/or approve amended or new versions of the Security Plan, and allow time for those revised arrangements to become embedded and operational with proven reliability prior to an increase in site sensitivity or categorisation. Examples of phases will be dependent on the function of the new facility, but may include:
- Ground Investigations.

² For the purposes of the TAG, 'physical' protection covers all aspects of protective security, including CS&IA and Personnel Security, both technical and procedural).

OFFICIAL

OFFICIAL

- Preparatory Groundworks.
 - Technical Galleries.
 - First Nuclear Concrete.
 - Bulk Mechanical, Electrical and HVAC (MEH).
 - Introduction of Nuclear or Other Radioactive Material.
 - First Criticality.
- 8.2 Consideration should also be given to the proportionate arrangements for Temporary Security Plans (TSPs) during the transitional period without them placing an unnecessary burden on both dutyholder and regulator. This may be achieved by defining in the Security Plan the type of activity and bounding cases where TSPs are required.

Coordination with Licence Application and Licence Grant

- 8.3 The ONR publication 'Licensing Nuclear Installations' requires appropriate measures to be in place to manage all aspects of security before a site licence is granted. Inspectors will be required to assess the security measures in place and confirm they are appropriate. The continued evolution of the documented arrangements, from the CSSP through to the Security Plan, should be regularly discussed between the developer/operator and the ONR regulator prior to the start of the site licence application period to ensure the version of the Security Plan to be formally submitted prior to site licence grant, meets regulatory expectations. This de-risks the site licence grant process. The dutyholder must submit a Security Plan at licence application and this must be formally approved by ONR prior to a licence being granted. This is formal acceptance that ONR is satisfied with the security arrangements in place at the time of licence grant, and is content with the plans and proposals for how these arrangements will be further developed at each phase of the project, up to, and after, operations have commenced.
- 8.4 While ONR does not expect a Nuclear Construction Site to have a fully mature Security Plan during the licence application stage, the expectation is that the GDA Security Concept of Operations is developed further into a CSSP and then into a framework SyAPs-aligned Security Plan. Certain 'strategic enabler' Fundamental Security Principles 1 to 5 will be of greater relevance during the early stages of the project as these are focussed on creating the right conditions to support high reliability security arrangements. ONR considers the 'secure operations' FSyPs 6 to 10 to be of increasing relevance as the project progresses as these are focussed on the implementation and maintenance of nuclear security and provide the regulatory framework for the development of an effective holistic security regime for the lifetime of the facility.

Inspectors should consider:

- Is the security phased in its approach to reflect the level of risk as the project progresses?
- Are there appropriate hold points identified between the phases?

OFFICIAL

OFFICIAL

- Are there appropriate provisions in place for engagement with the regulator to support achieving approval of the Security Plan as a pre-requisite for site licence grant?

9. SECURITY ARRANGEMENTS FOR A NUCLEAR CONSTRUCTION SITE (PRE-SITE LICENCE GRANT)

- 9.1 An approved CSSP must be in place before a developer undertakes activities on a nuclear construction site to construct a new nuclear facility and for which Planning or Development Consent has been granted. The CSSP for the construction phase (up to the point of site licence grant) should reflect the arrangements listed below.

Security Appointments

- 9.2 A Company Security Manager should be appointed at the early stages of the project to develop security arrangements and author the CSSP which will evolve into the Security Plan. A member of the dutyholder's senior management team should be appointed to oversee the overall delivery of security and represent the Security function at Board level.
- 9.3 A Suitably Qualified and Experienced (SQEP) Site Security Manager should be appointed to be formally responsible for all security activity at the site and act as a security focal point for liaison with the adjacent site.
- 9.4 Once appointed, the Construction Site Director and other senior staff with security responsibilities should have clear sight of security measures being adopted, a clear understanding of the risks and have clear responsibilities for security delivery and governance. The responsibilities and accountabilities of all staff with a security role must be documented.
- 9.5 In addition to site Security staff, there should also be a well-resourced strategic Security function, with adequate numbers of SQEP staff, which has responsibility for future planning arrangements as the site progresses from construction, through all transitional phases, to eventual operations.

Corporate Security

- 9.6 In addition to site Security staff, there should also be a well-resourced Corporate Security function, with adequate numbers of SQEP staff, which has responsibility for future planning arrangements as the site progresses from construction, through all transitional phases, to eventual operations. There should be effective integration and coordination between the Corporate Security function and other key functional areas, including Safety (C&I, Electrical, Civils etc), Design Authority, Assurance and Supply Chain. The Corporate Security function must be able to demonstrate that it has the capability and capacity to deliver the proposed security arrangements, in accordance with regulatory expectations, for the operational facility and during all transitional phases. These arrangements must be formally recorded in the ONR approved Security Plan. It is anticipated that the Corporate Security function would provide the framework for the 'strategic enablers' relating to SyAPs FSyPs 1 – 5, which provide the foundation for any capable and effective organisation.

OFFICIAL

OFFICIAL

Liaison with Adjacent Site

- 9.7 Arrangements must be in place between the Site Security Manager and the adjacent nuclear site's Site Security Manager to ensure there is regular liaison, effective communications including those relating to activity on site, any potential hazards and reporting of security incidents.

Identification of Vulnerabilities and Hazards

- 9.8 Using the UK Design Basis Threat (DBT), as a basis, and building on the work already conducted during the GDA process, an evaluation of the vulnerabilities and hazards should be undertaken to ensure adequate security arrangements are in place to mitigate the associated risks of construction projects. Examples of vulnerabilities may during the earlier phases of construction, include heavy plant/vehicles, explosives and charges (used in geotechnical surveys), scaffolding, ladders, heavy tools, fuel and chemicals, and large mounds of spoil and earth. Focus for threats during the construction phase (prior to NM on site) is to minimise the risk to the adjacent site (if within 5km) and to mitigate the malicious introduction of defects. Example mitigation measures are at Appendix A.

Access Control/Authorised Entry

- 9.9 The term Access Control is commonly used in relation to site, key areas or building access. It is likely that the initial stages of any development will be undertaken on open land where Public Rights of Way (PROW) are still in place and there may be no defined perimeter. In such cases, access to controllable areas, buildings, plant and equipment should be strictly managed to mitigate any vulnerabilities that the dutyholder has identified.
- 9.10 Once PROW have been closed, a perimeter fence or barrier should be erected to delineate the boundary of the Nuclear Construction Site.
- 9.11 Only authorised personnel and essential vehicles should be permitted access. Non-essential vehicles should be parked off the construction site and away from any adjacent nuclear site or facility. Access points should be kept to a minimum and this should be discussed and agreed with ONR Safety inspectors to ensure there is no conflict or contradictory advice given to the developer.

Security Control Point

- 9.12 A Security Control Point (SCP) should be established on the site at the designated vehicle/pedestrian access point. It should be staffed by security personnel and used to control and account for pedestrians/vehicles accessing and exiting from the construction site. This can act as a base from which security patrols are carried out and security documentation/records held. Where appropriate, similar SCPs may be located to control access to specific parts of the site or buildings.

Searches

- 9.13 A facility should be provided at the SCP(s) to carry out searches of personnel and vehicles to minimise the risk of the introduction of prohibited items and prevent unauthorised removal of items or information.

OFFICIAL

OFFICIAL

Contractors Security Arrangements

9.14 Contracts with third parties should clearly stipulate the security arrangements that are required. Security arrangements for Tier 1 contractors should be recorded in the contractor's Security Management Plan. Contractors are required to adhere to the same security arrangements as the dutyholder's staff unless specified otherwise, in which case any divergence in the arrangements should be formally documented. Arrangements involving the submission of Security Management Plans by contractors to the dutyholder should be approved by the dutyholder's Security Manager and underpinned by comprehensive audit and assurance arrangements. The use of such Security Management Plan does not absolve the dutyholders from being responsible or accountable for security, and statements to that effect should be clearly articulated in the dutyholder's Security Plan.

Personnel Security

- 9.15 Large scale construction projects present unique challenges for dutyholders due to the large workforce on site, the majority of whom will probably be contractors and sub-contractors, both long term and transient, employing a mixture of backgrounds and nationalities. The level of vetting checks required for staff, contractors and visitors on a Nuclear Construction Site will depend on access requirements (e.g. to SNI, site plans and construction plant) and their roles, such as security and senior management positions. FSyP 8 requires dutyholders to deliver the appropriate combination of recruitment checks and vetting to satisfy themselves of the honesty and integrity of potential employees.
- 9.16 The dutyholder must have a clear personnel security strategy which reflects the phased approach where security arrangements are commensurate with the level of risk as the project progresses. Use of zones or compounds should be considered where access should be limited to those personnel with higher levels of vetting/security clearance.

Security Culture

9.17 There may be particular challenges to fostering a good security culture amongst workers on a construction site due to the large numbers of people involved, the often transient nature of contractors and the limited exposure many will have had to nuclear security. It is imperative that the dutyholder implements a robust nuclear security culture from the very initial start of the project, and that this culture continues to be reinforced as the project progresses through all phases.

Inspectors should consider:

- Is there a Company/Corporate Security Manager and a member of the senior management team appointed who are responsible for the strategic planning and the delivery of security for the operational facility?
- Is there a SQEP Site Security Manager responsible for all security-related activity on the site and to act as the security focal point for liaison with the adjacent site?

OFFICIAL

OFFICIAL

- Does the Construction Site Manager have a clear understanding of the risks and have clear responsibilities for security delivery and governance?
- Are all security responsibilities and accountabilities for all Security staff formally documented?
- Are there effective liaison arrangements in place with any adjacent nuclear premises (within 5km of the construction site)?
- Has the UK DBT and other appropriate threat assessments 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, incorporating a security control point and searching?
- Is there adequate control and management of the supply chain?
- Is there a clear and effective personnel security strategy at both the corporate and the site level?
- Is there a clear and effective CS&IA strategy at both the corporate and the site level?
- Is there an effective strategy in place to foster a strong security culture from the initial stages of the project?

10. LICENCED NUCLEAR SITE UNDER CONSTRUCTION

- 10.1 Although not a legal term (as defined in NISR 03), 'Licenced Nuclear Site Under Construction' is used to describe a new site on which construction activity is being carried out, from the point at which a nuclear site licence is granted up to the time that the site becomes operational. A Licenced Nuclear Site Under Construction must have an ONR-approved SyAPs-aligned Security Plan in place. The Security Plan should build on the measures already detailed in the CSSP to address the full range of threats to NM, ORM and SNI detailed in the UK DBT. The dutyholder should submit a draft Security Plan at the start of the licence application process and engage with ONR inspectors during its development throughout the application process. The Security Plan should reflect the phased approach to the incremental increases in the security arrangements throughout the complete duration of the project from construction through to operations. Importantly, this should cover the transitional arrangements when one of the units is operational while the other unit(s) are still under construction, as this is the most complex period for security.
- 10.2 At each review point (often coinciding with agreed hold points), the dutyholder will be expected to provide additional details of the security arrangements for each of the subsequent phases of the project. These proposed arrangements will be reviewed by ONR at agreed points to ensure plans align with regulatory expectations. This periodic review process will provide ONR with the requisite degree of assurance that the dutyholder has a complete understanding of how the holistic security regime will be achieved at each phase of the project through to end-state, and have satisfactorily

OFFICIAL

OFFICIAL

detailed and appropriate plans of how to achieve this. It is appreciated that the level of evidence presented in the Security Plan to support the claims and arguments will continue to be developed and refined during the various phases of the project and this evidence will also be subject to regulatory review. Changes to the end-state security architecture will require submission of an amended or new issue of the Security Plan for approval.

- 10.3 The Security Plan must be formally approved by ONR as a mandatory pre-requisite to the granting of a nuclear site licence.

Identification of Vital Areas

- 10.4 Using the UK Design Basis Threat (DBT) as a basis, and the Vital Area identification (VAI) study conducted during the GDA process, a continuing evaluation of the key assets should be undertaken. The principles of a graded approach and defence in depth should continue to be applied to ensure increasing levels of protection for these key assets as the project progresses. The VAI will inform a study of the vulnerabilities and is fundamental in designing the Physical Protection System which will eventually be in place (prior to the arrival of NM/ORM on site.) Both the VAI study and the Cyber Security Risk Assessment should be reviewed on a regular basis to ensure all VAs continue to be evaluated and an appropriate PPS remains in place to achieve the outcomes detailed in SyAPs.

Introduction of Nuclear or Other Radioactive Material

- 10.5 As the project progresses there may be a requirement to introduce Nuclear Material (NM) and Other Radioactive Material (ORM) such as radioactive sources and new nuclear fuel before the facility becomes operational. The security arrangements to protect this material must achieve the required PPS outcome as detailed in SyAPs.

Site Boundary

- 10.6 A permanent fence should be in place which delineates the site boundary and excludes any public rights of way.

Serious Organised Crime and Police Act (SOCPA)

- 10.7 Once a nuclear site licence has been granted the site becomes a 'designated site' subject to the Serious Organised Crime and Police Act (SOCPA) 2005 s128 (Reference 10). Dutyholders are to demonstrate that enforcement of SOCPA can be implemented whenever necessary (e.g. the provision of a defined boundary, access control and clear signage).

11. MULTIPLE UNIT SITES

- 11.1 New nuclear power stations may consist of two or more operating reactors in close proximity to one another. The timeframe for operations may mean one or more units operating whilst others are still under construction. This is a very complex and high-risk phase of the project and presents challenges for the effective delivery of a holistic security regime. Security arrangements during this period must still achieve the appropriate PPS outcome for the operating reactor(s). Inspectors should be flexible

OFFICIAL

OFFICIAL

and engage with dutyholders to ensure that security arrangements, some of which may be temporary, continue to achieve the appropriate PPS outcome.

Inspectors should consider:

- Does the Security Plan adopt the phased approach?
- Does the Security Plan contain an adequate level of detail for the progressive, incremental security measures and arrangements for all phases of the project, from construction through to end-state operations?
- Does the Security Plan provide assurance to the regulator that the dutyholder has a comprehensive understanding of the practical application of the principles of VAI and KSyPP?
- Does the Security Plan identify the point at which the site is sufficiently developed to be vulnerable to the introduction of defects which may compromise the safety or security of the facility once it starts operating?
- Does the Security Plan demonstrate the required security outcome is achieved at all stages of project development, particularly as NM and ORM is brought on and the categorisation for theft and sabotage increases?
- Is there an appropriate site boundary in place that allows in enforcement of SOCPA once the licence is granted?

OFFICIAL

OFFICIAL

12. REFERENCES

1. **Security Assessment Principles.** <http://www.onr.org.uk/syaps/>
2. **Nuclear Industries Security Regulations 2003.** Statutory Instrument 2003 No. 403
3. **Convention on the Physical Protection of Nuclear Material (CPPNM)**
<https://ola.iaea.org/ola/treaties/documents/FullText.pdf>
4. **IAEA Nuclear Security Fundamentals.** <https://www.iaea.org/resources/nuclear-security-series>
5. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
6. **IAEA Nuclear Security Series No. 19.** Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1591_web.pdf
7. **HMG Security Policy Framework.** Cabinet Office.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf
8. **NISR 2003 Classification Policy** for the Civil Nuclear Industry (Nov 17)
<http://www.onr.org.uk/documents/classification-policy.pdf>
9. **The Anti-Terrorism, Crime and Security Act 2001.**
http://www.legislation.gov.uk/ukpga/2001/24/pdfs/ukpga_20010024_en.pdf
10. **The Serious Organised Crime and Policing Act 2005.**
http://www.legislation.gov.uk/ukpga/2005/15/pdfs/ukpga_20050015_en.pdf

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

OFFICIAL

OFFICIAL**13. GLOSSARY AND ABBREVIATIONS**

CPPNM	Convention on the Physical Protection of Nuclear Material
CSSP	Construction Site Security Plan
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	Nuclear Security Series
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PPS	Physical Protection System
PROW	Public Right of Way
SIA	Security Industry Association
SNI	Sensitive Nuclear Information
SOCPA	Serious Organised Crime and Policing Act
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide

OFFICIAL

OFFICIAL

APPENDIX 1 – SUMMARY OF INDICATIVE MEASURES FOR NUCLEAR CONSTRUCTION SITES

1. The table below provides details on the most commonly deployed measures and processes to achieve the required security for a nuclear construction site. It is not an exhaustive list and dutyholders may consider other measures that achieve the required outcome.
2. Each measure or process should be applied in a graduated manner according to the threat or risk being mitigated as the site develops.

MEASURES AND PROCESS TABLE – NUCLEAR CONSTRUCTION SITES	
Measure or Process	Description
Prevent Unauthorised Access to equipment	<p>Initial stages - Site will not have a perimeter.</p> <ul style="list-style-type: none"> • Account for all personnel on site. • Remove or secure all equipment and plant which pose a threat to the adjoining site(s) when not in use such as ladders, scaffolding, hazardous material in compounds, stores or ISO Containers. • Ensure keys are adequately secured and controlled • Clearly define any trespass policy and how the company will deal with trespass and protest action • An inventory of equipment should be kept and frequent checks carried out • When Public Rights of Way are closed/re-routed, install a suitable fence to define the perimeter and provide for a defined site access/exit point(s)
Plant and Vehicles	<ul style="list-style-type: none"> • Construction sites should not be used as storage areas when plant is not in use and the amount of plant on site should be minimised. • Designated compounds or parking areas, away from the adjacent site, should be used when plant is not in use. • Plant and vehicles should be immobilised when not in use. • Keys should be controlled and drawn only by authorised persons
Spoil	<ul style="list-style-type: none"> • Extensive excavation work will result in large quantities of spoil. A plan should be in place to address the impact of spoil mounds on security measures facilitating an attack or the conduct of hostile reconnaissance on an adjacent operating facility, or circumvent security measures

OFFICIAL

OFFICIAL

MEASURES AND PROCESS TABLE – NUCLEAR CONSTRUCTION SITES	
Measure or Process	Description
Liaison with other adjacent Site	<ul style="list-style-type: none"> • Ensure formal liaison takes place with security staff from adjacent sites (within 5km) and stakeholders such as CNC and Home Office Police force CTSA's. • Appropriate arrangements should be in place to report security incidents to the company security manager and adjacent nuclear site's security staff on a 24/7 basis
Maintain Clear Zones	<ul style="list-style-type: none"> • Ensure clear zones are maintained around site and adjacent sites • Ensure non-essential vehicles are parked off-site and well away from any adjoining nuclear facility.
Guarding/Security Force	<ul style="list-style-type: none"> • A SQEP security force should be in place. Duties should be clearly documented. Where CGF are employed, contracts should include a set of key performance indicators. • Contract guards must be SIA Licence holders. • A Security Control Point should be located by the access point.
Prevent prohibited items being introduced to site	<ul style="list-style-type: none"> • Random searches of personnel/vehicles entering site should be carried out to achieve the specified security outcome.
Contingency Plans	<ul style="list-style-type: none"> • Contingency plans should document actions to be taken if a security event, including protest action takes place. This should include communication with CNC, local police and adjacent sites
Personnel Security	<ul style="list-style-type: none"> • Clear policy should document the requirements for background checks

OFFICIAL

OFFICIAL

APPENDIX 2 – SUMMARY OF INDICATIVE MEASURES FOR CIVIL LICENCED NUCLEAR SITES UNDER CONSTRUCTION

1. A Civil Licenced Nuclear Site Under Construction must have an approved Security Plan. The Security Plan may be a simple transition from the CSSP, but a phased approach should be adopted. The Security Plan relating to the operational site should reflect the appropriate PPS outcome and the relevant TAGs should be referred to. Similarly, the relevant PPS outcomes must be achieved from the point at which NM and/or ORM is introduced to the licenced site.

MEASURES AND PROCESS TABLE – CIVIL LICENCED NUCLEAR SITE UNDER CONSTRUCTION	
Measure or Process	Description
Prevent Unauthorised access to Site	<ul style="list-style-type: none"> • Ensure a site perimeter is in place, all PROW are closed and clear zones are in place around perimeter. • All personnel entering site are authorised through checks by guard force or use of AACS • Vehicle access limited to essential vehicles and minimised with the use of off-site delivery points. • Vehicles are searched on entry
Contingency Plans	<ul style="list-style-type: none"> • The dutyholder is to ensure appropriate contingency plans are in place to assist in countering relevant malicious capabilities. These should be consistent with emergency arrangements. In particular, dutyholders should recognise the potential increase in threat from protestor action.
Prevent unauthorised access/use of equipment	<ul style="list-style-type: none"> • Plant/vehicles should be immobilised and cabs should be secured when unoccupied. • Use of PIN protected control systems should be considered. • Vehicles should be parked in designated positions away from adjacent or sensitive areas. • Consider use of Vehicle alarms/tracking systems • Secure Compounds/ISO Containers used for ladders, scaffolds, hazardous materials etc. • Ensure there is an inventory of plant, equipment, volatile materials and that random checks are carried out on them. • Keys should be held securely and accounted for at all times. • Access controls should prevent unauthorised persons accessing equipment or plant.

OFFICIAL

OFFICIAL

<p style="text-align: center;">SOCPA Provisions</p>	<p>SOCPA is very specific on what parts of a licenced site are covered as detailed below:</p> <ul style="list-style-type: none"> • all ground inside the outer perimeter of the protection required for any premises, defined as the line of the outermost fences, walls or other obstacles provided or relied upon for protecting those premises from intruders; and • that line shall be determined on the assumption that every gate, door or other barrier across a way through a fence, wall or other obstacle is closed. <p>How this is managed is a matter for dutyholders, however as a minimum the following is to be achieved:</p> <ul style="list-style-type: none"> • warning signs are displayed around the outer perimeter to ensure all possible approach routes are adequately covered, especially those that adjoin public property and rights of way; • wherever possible, signs are located so they can also be read during the hours of darkness; • signs are made and, where practicable, positioned in such a way that reduces the possibility of them being used as climbing aids, but ensures that they are securely attached to a fence; • signs are positioned so that, wherever possible, lines of sight/vision through a fence are kept clear; • sufficient spare signs are held to replace any lost or damaged; and, • procedures are in place to liaise with civil police.
<p style="text-align: center;">Tower Cranes</p>	<ul style="list-style-type: none"> • Arrangements should be in place to secure the base of a tower crane effectively. • The span of the crane should not compromise security of an adjacent site or operating reactor's perimeter. • On a multi-unit NPS, construction requiring tower cranes should be completed before any adjacent unit operations commence.
<p style="text-align: center;">Void Management</p>	<ul style="list-style-type: none"> • As the build progresses, the complexity of structures will increase. To minimise the risk of unauthorised items being introduced, dutyholders should have documented arrangements that cover the security of voids in structures. This should include a means of searching then securing voids. • Zoning of sites to protect critical infrastructure.

OFFICIAL

OFFICIAL

Technical Security Measures	<p>Construction sites may cover a wide area several times the size of the eventual operating site. Electronic security arrangements such as PIDS, CCTV, AACS and lighting should be considered and deployed as is practicable. When identifying vulnerabilities, dutyholders should have prioritised where the deployment of such systems will be most effective. The following should be taken into account:</p> <ul style="list-style-type: none">• Sites may not have an electricity supply, therefore equipment with self-contained power sources – diesel generators, battery supplies, solar and wind powered should be considered.• The continuous development of the site should be taken into account and portable security systems may need to be considered.• Site activities should be taken into account with regard to cable laying, particularly when heavy plant is moving and excavations are underway. Consideration may be given to alternative transmission systems such as wireless technology.• Where PIDS/IDS are used, there should be a suitable means of verification/assessment in place.• An OR1 and OR2 should be completed to determine what security measures are needed and to what effect.
------------------------------------	---

OFFICIAL