ONR GUIDE			
PHYSICAL PROTECTION OF INFORMATION			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-7.4 Revision 0		
Date Issued:	April 2017	**Review Date:**	April 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19077. (2017/110601)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/17

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). 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 1).

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 (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR Inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's arrangements for the physical protection of information and information assets. 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, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 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.

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 CS&IA 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 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle L of the CPPNM refers to confidentiality and details that the State should establish requirements for protecting the confidentiality of information, the

unauthorised disclosure of which could compromise the physical protection of nuclear material and nuclear facilities. The importance of issues relating to CS&IA is also recognised 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:

  g) Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.

  h) Ensure that prime responsibility for the security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets rests with the authorised persons.

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:

  h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2). Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

4.4 The IAEA also publishes Implementing Guide NSS No. 23-G 'Security of Nuclear Information' (Reference 8) and Technical Guidance NSS No. 17 'Computer Security at Nuclear Facilities' (Reference 9).

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 Security Delivery Principle 7.4 – Physical Protection of Information and Information Assets, in support of FSyP 7 – CS&IA. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) 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 Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise data in various formats (such as digital, hard copy and knowledge) as well as information technology and operational technology (equipment or software). It is a dutyholder's responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI and computer based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilised on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should always be considered. Appendix 1 of TAG 7.2 provides a description of SNI and a flow chart to assist in its identification.

6.2 The physical protection of information and associated assets is one of the four cornerstones of information security - together with technical, personnel and procedural measures. As such, physical security complements the others and is part of a holistic layered security approach that mitigates the identified risks.

6.3 Inspectors should assure themselves that physical security measures are adequately supported by procedural and in some cases personnel security measures. Effective physical protection of information and associated assets encompasses all relevant aspects of:

- Physical security risk assessment
- Physical security control measures
- Assurance of physical control measures

Regulatory Expectations

6.4 The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements for the physical protection of information and associated assets in support of maintaining effective CS&IA arrangements.

FSyP 7 - Cyber Security and Information Assurance	Physical Protection of Information	SyDP 7.4
Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.		

7. PHYSICAL SECURITY RISK ASSESSMENT

7.1 Inspectors should gain assurance that a comprehensive physical security risk assessment has been undertaken. The scope of the assessment should be clearly defined and should derive some of its input from the work to identify and classify information and associated assets (see TAG 7.3 Protection of Nuclear Technology and Operations for further guidance). The purpose of the risk assessment is to ensure that all relevant risks are identified so that they can be managed effectively in the context of

the business. If the risk assessment is conducted early in the process to deliver new capabilities or upgrades to existing facilities, then physical security can be built in at the outset which is far more effective.

7.2 Where information and associated assets are located on nuclear premises, it is highly likely that a comprehensive site physical security assessment will already have been completed to assess the risk of malicious acts to Nuclear Material (NM), Other Radioactive Material (ORM) and nuclear facilities. This should have resulted in a comprehensive physical protection system designed to protect those assets for which the dutyholder is responsible. This risk assessment should fully consider acts of both theft and sabotage and therefore controls to mitigate these threats should already be in place for the NM/ORM and the site (Refer to SyAPs FSyP 6, the associated SyDPs and TAGs for further guidance). Accordingly, for nuclear premises, the risk assessment for information and associated assets should sit within the context of the overall site physical security assessment.

7.3 The initial stage of the assessment should be to develop a specification such as an Operational Requirement Level 1 report in line with the CPNI Guidance to Producing Operational Requirements (Reference 11). This should capture the scope, the physical security measures currently in place, any vulnerabilities and determine what the requirements should be.

7.4 Information and associated assets may include data centres, data storage systems, IT system management areas, communications systems and their components, IT peripherals used to hold information, hard copy storage areas, removable media (and their associated physical transfer mechanisms), mobile devices of all types, and relevant supporting infrastructure.

7.5 There are a number of methodologies and tools for conducting a physical risk assessment and dutyholders should employ a mechanism that they feel is appropriate to their context. CPNI advise the use of the Classified Material Assessment Tool (CMAT) which considers risks from surreptitious attack. CMAT is available from the CPNI extranet website. Whichever mechanism is used the risk assessment should consider the following:

- Surreptitious and forced attack
- Personnel, all staff and visitors
- Disposal of information storage devices and containers – to include peripherals such as printers
- Remote and mobile working (e.g. loss or theft of mobile devices)
- Removable media and other forms of data transfer (e.g. hard copy transfers)
- Natural and environmental hazards. For example the server room should not be located in a basement if there is a naturally high water table in the area

7.6 These risks should take account of business impact assessments conducted as part of Business Continuity and Disaster Recovery planning.

Inspectors should consider:

- Are the physical security measures part of a layered approach based upon a risk assessment?
- Does the risk assessment adequately consider all relevant threats?
- Has an appropriate specification (such as an Operational Requirement) been produced and used to design the physical protection of information and associated assets?

8. PHYSICAL SECURITY CONTROL MEASURES

8.1 The risk assessment should inform a plan to mitigate the risks. A physical security plan or similar should be used to summarise what measures are required, how they should be implemented and how assurance should be provided and maintained.

8.2 The types of controls that could be in place to mitigate physical security risks should include, but not be limited to, those listed in the sections below. The inspector should be able to see a clear link between risks and why particular controls are specified. Dutyholders should consider controls that will deter, delay, detect and respond to physical risks, including those posed by insiders.

8.3 Physical security measures should be deployed in a defence in depth approach that provides layers of protection. The risk assessment should enable controls to be implemented in a proportionate manner focussed on the most sensitive assets.

Building and Room Security Measures

8.4 Physical segregation measures should be in place such as controlled entry/exit/access and egress points for buildings, rooms and more vulnerable specialist areas using walls, floors, ceilings, doors and windows. Where such control measures are deployed, their primary purpose, for example, to delay forced attack or to deter and detect surreptitious attack, should be clearly defined in the physical security plan.

8.5 The technical specification of physical measures such as walls and windows can be reduced in some cases if they are supported for example, by alarms linked to sensors and if the response from a guard force or authorised user is adequate.

8.6 Where secure rooms have been defined, the requirements for environmental management such as temperature control, ventilation and humidity should be taken into account.

8.7 Such areas should also specify fire detection and control mechanisms linked to a monitoring alarm and appropriate response such as fire suppression and the fire brigade.

8.8 Automated Access Control Systems (AACS) with proximity passes are a common physical security control for buildings and rooms and consideration should be given to compartmentalised configuration of such systems to ensure that personnel only have access to areas for which they have a need to go.

8.9 Each AACS should also have a comprehensive management process in place to authorise accounts on the system and to either change access as personnel change roles or to remove access as soon as it is no longer required.

8.10 Additional security controls (physical, personnel, procedural and technical) should be considered for the staff and technology that manage aspects of the AACS (for example production of tokens).

Alarms

8.11 Alarm systems should be considered for monitoring access to those rooms and areas and communications pathways, where information and associated assets may be stored or processed. Alarms are intended to alert for an intrusion event and should be used in concert with a response function (e.g. guard force or authorised users).

8.12 Alarms should be of an approved type (see CPNI and commercial good practice guidance) using sensors and triggers appropriate to the environment being protected. Appropriate controls should be applied across all maintenance and management aspects of the system to ensure functionality. Inspectors should review if alarm systems are adequate in terms of coverage, purpose and implementation.

8.13 Procedural controls are fundamental for responses to alarm activations and dutyholders should ensure that authorised personnel are available to respond to alarms in a timely manner by such means as; call out lists, key holder rotas and clear responsibilities.

8.14 If first response to a security alarm activation is an on-site guard or police force, then its responsibilities should be made clear e.g. under what circumstances are they to enter the area or are they to remain outside and call an authorised user?

CCTV

8.15 A CCTV system can be an effective protection mechanism for both internal and external use. This is a specialist subject and any installation should consider a variety of factors, the primary one being what is the system intended to achieve, e.g. facial recognition, alarm assessment, night operation etc.

8.16 CCTV should be monitored appropriately based upon whether the function is real time surveillance or for historic recording to be made available for review subsequent to a security event. Dutyholders should have a clear understanding of what the system is intended to do and why. CCTV should be monitored by Suitably Qualified and Experienced (SQEP) personnel.

8.17 CCTV systems are vulnerable to attack and dutyholders should consider risks such as cables being compromised physically, cameras being obscured, remote control systems being taken over by hackers and signals intercepted and diverted elsewhere.

8.18 Data retention is a significant factor for CCTV systems and issues to be considered include how much data will be stored, in what format, where, and for how long. A significant aspect is access control to the data, to include legal obligations under the Data Protection Act and the preservation of potential forensic evidence.

Guard Force Training

8.19 Many physical security measures rely upon human intervention to respond to alarms to prevent unauthorised access or damage to information and associated assets.

Dutyholders should ensure that guard forces have clearly defined responsibilities and are SQEP for their roles. TAG 9.3 - Security Guard Services covers this topic in more detail.

8.20 This is especially the case where guard or reaction forces are provided by a commercial company. In this case quality performance criteria should be part of Service Level Agreements (or similar) and these should also specify redress procedures in the event of poor service or other failures to meet contract requirements.

Secure Containers

8.21 Containers may be required even within defined secure areas to protect hard copy SNI or to provide additional protection to sensitive data stores and system components such as servers. Such measures can be used to counter the threats from insiders, visitors and other personnel in the environment. Details of approved security furniture and equipment can be found in the CPNI Catalogue of Secure Equipment.

Equipment Siting

8.22 Technology should be sited in a manner to mitigate the risk of overlooking and overhearing from personnel without a need to know. In many modern buildings an open plan environment is favoured but this must be balanced by maintaining the need to know where SNI is potentially at risk.

8.23 Suitable measures and processes (physical and otherwise) should be considered for meeting rooms and other communal areas (including staff restaurants) where overhearing or eavesdropping may be a risk to managing access to SNI or as a minimum, to preserving need to know. Siting of conferencing equipment may also give rise to risk of overseeing/overhearing or eavesdropping, particularly where it is capable of being remotely operated.

Cable Security

8.24 Dutyholders should assess the risks to cables running through working areas and measures should be considered to prevent unauthorised access or physical damage (accidental or deliberate). The decision to use a particular network cable type (e.g. fibre, copper or coaxial) for technology has a security dimension in addition to capacity and functionality requirements.

8.25 Cable security should be maintained so that cable runs for secure systems are either segregated (using locked but inspectable trunking) or differentiated (e.g. different colour cables or labels) as appropriate. This is a matter not only of good housekeeping from a support perspective, but is also a system segregation measure that contributes to system resilience.

8.26 Dutyholders should take account of the possibility of crosstalk between systems of different security sensitivity with long parallel cable runs, especially when they are in close proximity in shared trunking. IT/OT cables for systems carrying SNI should not routinely be in the same trunking as power cables.

TEMPEST

8.27 The level of TEMPEST threat within the UK is assessed as being NEGLIGIBLE, except in large cities. Most locations hosting information and associated assets should, by

their very nature, have extensive controlled space around them which should prevent some types of TEMPEST attack. This is not the case for all locations however and dutyholders should consider TEMPEST compromise methods in their risk assessments and implement measures as appropriate.

8.28 Dutyholders should implement measures to avoid or reduce crosstalk between systems operating with SNI and those of different security sensitivity. Furthermore, dutyholders should implement measures to prevent interference or crosstalk where the cables of systems with SNI are unavoidably close to system power lines. Such measures could include filtering of mains power.

Control of Removable Media

8.29 Where media (of all types) is used to transfer SNI, physical security risks to include loss and/or theft of such media should be mitigated.

8.30 Protection of removable media (USB devices, flash drives, CD/DVD, backup tapes) in transit can be achieved effectively using hardware and software controls (e.g. using suitable encryption products). Physical protection measures could include packaging, transit cases, escorting and courier companies. Dutyholders should ensure that the reasons for data transfer are clear and that SNI is protected adequately.

Remote Working & Mobile Devices

8.31 Where remote working is required operationally, dutyholders should have a clear understanding of the risks involved and should have measures in place to mitigate them adequately, supported by a mobile working policy.

8.32 Since mobile devices are often used in less secure environments, the physical security aspects of device storage should be considered both in transit (e.g. in a car or train) and at rest (e.g. in a user's house or hotel environment). A number of layered security measures should be implemented (such as device secure configuration and encryption) to protect mobile devices and remote connections. Physical measures could include secure containers and tethering mechanisms. Dutyholders should be able to demonstrate that the risks are understood and have been mitigated to an adequate extent.

Secure Disposal of Assets

8.33 Information and associated assets should be sanitised adequately for re-use or destroyed securely when no longer required. This applies to both hard copy and digital information however stored. Advice on appropriate sanitisation techniques and destruction mechanisms is available from the NCSC and the Centre for the Protection of National Infrastructure (CPNI). Sanitisation or destruction mechanisms must be supported by an appropriate tracking and recording mechanism to provide traceability of information and associated assets at all stages. Where information and associated assets have been physically destroyed a destruction certificate should be provided where appropriate.

8.34 Commercial tools are available for secure sanitisation and NCSC provide guidance on these together with a certification service for approved products. Similarly, commercial companies can gain certification to required standards to demonstrate that they are qualified to conduct various types of secure destruction.

8.35 Secure destruction should be applied to all types of information assets – including hard copy and guidance on appropriate shredders for paper documents is available from the NCSC and CPNI.

8.36 Inspectors should confirm that consideration has been given to SNI stored on rented equipment such as printers or multi-functions devices. Rental contracts for such devices often require the return of out of date equipment intact so that it can be replaced with newer versions. Care should be taken that the equipment has been sanitised adequately before it is returned to the commercial provider.

Environmental Controls

8.37 SNI will be stored in a variety of locations and systems within dutyholder organisations and the environmental controls for all of these locations should be considered to ensure that information and associated assets are not damaged or destroyed by changes in conditions. Technology may be susceptible to extremes of temperature and humidity, whilst information in hard copy is vulnerable to damage from excess humidity and flooding.

8.38 Environmental controls are often managed through Building Management System software and while that is often a pragmatic and cost effective solution, inspectors should gain assurance that dutyholders have taken into account relevant factors such as any single points of failure or vulnerabilities of sensors/remote management systems to cyber attack.

8.39 Electrical equipment storing or processing SNI may be vulnerable to changes in electricity supply such as power fluctuations and total supply failure. Dutyholders should make provision for such eventualities and have mechanisms in place to mitigate these risks using un-interruptible power supplies and other solutions.

8.40 There will be many critical systems on a dutyholder's site that will require a constant power supply and inspectors should confirm that information assets operating with SNI are included in that consideration.

Inspectors should consider:

- Has a physical security plan or similar been developed to describe the controls in place and is it appropriate?
- Are physical security measures for buildings, rooms and containers appropriate for the level of risk?
- Where AACS systems are in place have measures for their protection been implemented?
- Are area alarms of an adequate standard and are they monitored appropriately?
- Is the alarm response force trained and resourced adequately to respond to physical security events that affect SNI?
- Has the purpose of CCTV systems been clearly defined and is the technical implementation adequate?
- Has consideration been given to siting of technology?
- Is cable layout and security part of a planned and structured process?

- Have TEMPEST considerations for the site been assessed and mitigated adequately where appropriate?
- Is there evidence that secure disposal mechanisms are being implemented?
- Have any risks to the operation of environmental management systems been identified and mitigated adequately?

9. ASSURANCE OF PHYSICAL SECURITY MEASURES

9.1 As with all security controls, assurance is required that they are effective both on implementation and throughout the lifetime of the information and associated asset. Accordingly, dutyholders should have a mechanism in place to provide appropriate assurance.

9.2 Dutyholders should recognise that threats, technology and business functions all change over time and have mechanisms in place to monitor these changes and react accordingly. TAG 7.1 – Effective Cyber and Information Risk Management describes the requirement for a risk management process managed by a security governance structure and physical security should be part of that approach. Physical security measures and their associated management should be able to respond quickly to a change in threat or to an event and scale up so that existing controls can be expanded and/or augmented by additional measures. Such measures could include for example additional personnel, increased monitoring, introducing exit searches or increased CCTV coverage. Further information on assurance and how it fits within a corporate governance structure can be found in TAG 1.1 - Security Governance and Leadership; and, TAG 1.5 – Security Assurance Processes.

9.3 Physical security considerations should be an intrinsic part of the change management function so that the distinctive issues around it can be taken into account when site and system changes are being discussed.

9.4 Dutyholders should have a maintenance programme for equipment such as alarms, CCTV and containers to ensure that they remain effective. Further guidance on these issues can be found in TAG 5.2 – Examination, Inspection, Maintenance and Testing of Security Equipment.

Contractor Management

9.5 Dutyholders are responsible for managing risks to their information and associated assets held within their supply chain. They should therefore approve the physical security (and other security) measures implemented by their contractors. This approval should take account of the requirements in the SPF, as qualified by the relevant FSyPs and relevant good practice.

Inspectors should consider:

- Is there adequate assurance that physical security measures are effective?
  - Is there a process for monitoring and for identifying and addressing deficiencies?
- Is there confidence that changes to threats, technology or the business are reflected in a review of security measures as part of the change management process?

- Is there assurance that physical security measures can be scaled up as necessary?

- Are all physical security measures adequately supported by procedural and personnel measures?
- Does the dutyholder ensure that risks to SNI held within its supply chain are appropriately managed?

10. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

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. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **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

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

7. **Security Assessment Principles** – Trim Ref. 2017/121036

8. **IAEA Nuclear Security Series No. 23-G**. Security of Nuclear Information http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf

9. **IAEA Nuclear Security Series No. 17**. Computer Security at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

10. **NCSC - A Critical Appraisal of Risk Methods and Frameworks** https://www.ncsc.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks

11. **CPNI – GUIDE TO PRODUCING OPERATIONAL Requirements for Security Measures** **HTTPS://WWW.CPNI.GOV.UK/SYSTEM/FILES/DOCUMENTS/D5/76/GUIDE-TO-PRODUCING-OPERATIONAL-REQUIREMENTS-FOR-SECURITY-MEASURES.PDF**

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

11. GLOSSARY AND ABBREVIATIONS

AACS	Automatic Access Control System
CMAT	Classified Material Assessment Tool
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
IT/OT	Information Technology/Operational Technology
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide