Physical Protection of Information			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-7.4	**Issue No.:**	2
Record Reference:	2022/16014		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-26
Prepared by:		Inspector Cyber Security & Information Assurance	
Approved by:		Professional Lead Protective Security	
Professional Lead:		Professional Lead Cyber Security & Information Assurance	
Revision Commentary:	Planned routine review. Amended to align to revised National Technical Authority relevant good practise, ONR and HMG policy documents, and ONR TAG template format amendments.		

Table of Contents

1. Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.

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. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR 2003') [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] 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 TAG is such a guide.

2. Purpose and Scope

3. 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 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 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 UK Legislation and Policy

4. 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.

5. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR 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.

6. 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 7.4 – Physical Protection of Information, in support of FSyP 7 – Cyber Security & Information Assurance. This TAG is consistent with other TAGs and associated guidance and policy documentation.

7. The Government Functional Standard on security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties.
The security principles, governance, life cycle and practices detailed within the Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

8. The Government Security Classifications document, together with the ONR Classification Policy [4] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

4. Relationship to International Standards and Guidance

9. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals [6]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

10. 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.

11. A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13 [7]. Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

12. The IAEA also publishes Implementing Guide NSS No. 23-G [8] and Technical Guidance NSS No. 17 [9].

5. Advice to Inspectors

13. 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 and hard copy) 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 CNS-TAST-GD-7.2 [10] provides a description of SNI and a flow chart to assist in its identification.

14. Controls are the primary components to consider when developing an information security strategy and can be physical, technical or procedural. The choice of controls must be based on a number of considerations including ensuring their effectiveness in mitigating assessed risks and what the optimal form the control will be.

15. 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

16. This TAG draws heavily on Relevant Good Practice (RGP) provided by CPNI and NCSC as the National Technical Authorities (NTAs). Other sources of RGP which support the physical protection of information includes, but is not limited to, international standards such as International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 27001 [11] and IEC 62443 [12], the Information Security Forum (ISF) Standard of Good Practice for Information Security, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Advice and guidance on a risk assessment approach and methodology can be found in CNS-TAST-GD-7.1 [13].

6. Regulatory Expectation

17. 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

18. Physical and environmental security controls for the protection of SNI should be applied according to layering principles and based on a risk assessment to determine applicable threats and risks in line with guidance set out by CPNI.

19. 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 CNS-TAST-GD-7.3 [14] 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.

20. 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.

21. The risk assessment should also reflect the insider threat and consider the unique problem this poses due to the advantages they have over an adversary that does not have authorised access, as described in CNS-TAST-GD-11.4.2 [15], CPNI guidance [16] and other RGP in this area, when mitigating the associated risks.

22. The initial stage of the risk assessment should be to develop a specification of the organisation’s needs. CPNI promote their Operational Requirements (OR) process as a tool to enable an organisation to produce a clear, considered and high-level statement of their security needs based on the risks they face and leads to the application of effective and proportionate protective security measures. CPNI recommends completing both a risk assessment and their OR used in line with the CPNI Protective Security Risk Management [17] and CPNI Guidance to Producing Operational Requirements [18], respectively, as an essential part of any security project.

23. Information and associated assets in scope may include data centres, data storage systems, IT/OT system management areas, communications systems and their components, Security Management Systems (SMS), workstations, IT peripherals used to hold information, hard copy storage areas, removable media (and their associated physical transfer mechanisms), mobile devices of all types, peripherals (such as printers) and relevant supporting infrastructure, both within the context of office/site and remote/home working environments. The CPNI Asset Identification Guide [19] has been developed to assist anyone responsible for identifying an organisation's critical assets as part of the Protective Security Risk Assessment process.

24. The threat vectors relevant to any given asset should be informed through the conduct of a protective security risk assessment. 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. To specifically consider the risks from surreptitious attack – carried out by a party who wishes to gain access to classified material for nefarious reasons to steal information, deny service, install malicious software, etc without being detected or leave any indication that an attack has taken place – CPNI advise the use of the Surreptitious Threat Mitigation Process (STaMP) [20].

25. Whichever mechanism is used the risk assessment should consider the following:

- The threat – including surreptitious and forced attack.
- Personnel, all staff and visitors.
- Information lifecycle from creation and receipt through to disposal of information and storage devices.
- New working arrangements – remote/home and mobile working.
- Removable media and other forms of data transfer.
- Natural and environmental hazards.

26. 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, and are these derived from credible threat information/intelligence?

- Has the dutyholder applied their chosen risk assessment methodology correctly?
- Has the risk assessment been reviewed periodically to confirm the controls in place are commensurate with the threat?
- Are risks defined and mapped to the areas under consideration?
- Has the dutyholder identified and developed a suite of protective security recommendations to address the risks?
- Has an appropriate specification (such as an Operational Requirement) been produced and used to design the physical protection measures for information and associated assets?
- Has an assessment of protective security recommendations (in terms of likelihood of success) been made?
- Have the risks been mitigated by the measures implemented? Is the residual risk acceptable?
- What processes are in place to identify changing threats and to scale up physical security if/when necessary?

8. Physical Security Control Measures

27. 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.

28. The types of controls that could be in place to mitigate physical security risks should include, but not be limited to, those listed in Appendix 1, 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, assess and respond to physical risks, including those posed by insiders.

29. 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.

30. For these physical security elements to be effective, they must be supported by a Suitably Qualified and Experienced Person (SQEP) and enforced by appropriate standards, procedures and arrangements. Training or guidance must also be provided to enable staff to implement, use and manage physical security controls correctly and where appropriate recognise, react to and report signs of a possible attack.

8.1. Equipment Siting

31. 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.

32. 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.

8.2. Cable Security

33. 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. Consideration should be given to network patching security, and the physical

control of network ports in office areas and in data cabinets, and the implementation of controls around physical switch ports.

34. 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 resilience.

35. 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.

36. Sites should determine the potential impact of the consequences of malicious or non-malicious damage to the exposed cables on the security infrastructure (see paragraphs 55-56).

8.3. TEMPEST and Electromagnetic Security (EMS)

37. 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/EMS attack. This is not the case for all locations however and dutyholders should consider TEMPEST/EMS compromise methods in their risk assessments and implement measures as appropriate to manage the level of unintentional signals emanating from IT which may expose SNI.

38. Dutyholders should implement measures to prevent 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 or use of shielded cabling.

39. Dutyholders concerned about the exploitation of Electromagnetic (EM) signals around data security classified above OFFICIAL-SENSITIVE can request support from NCSC, as the NTA for TEMPEST and EMS, for consultancy, vulnerability assessments and operational assurance services [21]. ONR can also engage with the UK National Authority for Counter Eavesdropping (UK NACE) where deemed appropriate.

8.4. Control of Removable Media

40. Where media (of all types) is used to transfer SNI, physical security risks including loss and/or theft of such media should be mitigated. Dutyholders should limit the use of all removable media devices except when specifically authorised. An inventory of removable media should be maintained to

determine the location of assets and identify which individuals have access to them. Personal/unapproved removable media devices should never be used on official systems.

41. 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. NCSC provide Device Security Guidance on how to use peripherals securely [22].

8.5. Remote/Home Working and Mobile Devices

42. Where remote/home 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 remote/home working policy. 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 vehicle or train) and at rest (e.g., in a user's house, accommodation such as a hotel, or public places).

43. 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. Vigilance at all times and equipment siting, as described above, when using a mobile device, are important considerations to ensure that a conversation during conference/phone calls and meetings cannot be overheard and screen data cannot be seen – through physical positioning or the use of privacy screens – by others in these environments.

44. CPNI encourages the undertaking of a Personnel Risk Assessment for remote working to identify and address concerns [23], whilst further guidance can be found on the NCSC website [24].

8.6. Secure Disposal of Assets

45. Information and associated assets should be sanitised adequately for re-use or destroyed securely using appropriate equipment 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 [25], CPNI [26] and other RGP. 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.

46. 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. The use of mobile paper destruction service providers does not comply with CPNI's secure destruction standard regarding the particle sizes media should meet for above OFFICIAL. In some circumstances it may be more appropriate for an organisation to use mobile paper destruction techniques on their establishment compared to fixed site destruction techniques, which results in material being transited prior to being destroyed. NCSC guidance states that consideration to the geographic distance, in terms of the stops suppliers' vans have to make enroute, introduces risks which must be managed (for example using the 'two-person rule').

47. Inspectors should confirm that consideration has been given to SNI stored on rented equipment such as printers or multi-function 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. Where destruction or sanitisation doesn't take place on premise the classified contracts process should be considered in line with CNS-TAST-GD-7.2 [10].

48. In some instances, SNI may be retained for an extended period of time due to the lifecycle of the asset it relates to. A lack of dedicated document storage space at a facility may cause a dutyholder, or even their supply chain partner, to procure the services of an off-site archiving company. Under such circumstances, an assessment should be undertaken to ensure that the archiving company has suitable security arrangements in place to protect SNI in transit and in storage at their facility. The assessment of the archiving company should consider the classified contracts process in line with CNS-TAST-GD-7.2 [10].

8.7. Security Management Systems – Protection and Resilience

49. The increasingly sophisticated nature of IT systems and networks associated with SMS provides increased functionality in managing a site's physical security regime, but also introduces opportunity for a malicious threat actor, particularly an insider, to disrupt its service, potentially as part of a blended attack scenario. The physical protection of core components of the system represents one of several control areas CPNI consider in their Cyber Assurance of Physical Security Systems (CAPSS) standard that need to be implemented to protect against identified threats [26].

50. These include: disabling non-operational physical interfaces to prevent the exploitation of insecure internal or external interfaces; installing tamper alarms to prevent access to structures inside the tamper-protection boundary of the device; the protection of security related physical structures to prevent physical compromise of the device and unauthorised physical access to

security critical data stored on the device; and physical security of management interfaces to prevent their physical compromise. It also highlights that users should confirm the behaviour of the device on power loss to ensure that in the event of power failure the system cannot be exploited if the device fails or restarts in a way that undermines the device's security.

51. Power supply, and more significantly its back-up provision, is an important resilience feature and can be defined as an essential service critical to the operational process of the SMS to enable it to maintain the security infrastructure of the site. Other essential services may include communications, IT systems and infrastructure (including associated server rooms and cable infrastructure), and potentially air-conditioning systems.

52. The identification of single points of failure (SPOFs) in the SMS network topology or essential services supporting the SMS is vital as their loss would cause the functionality of the SMS to cease or be unacceptably impaired. It relies on the concept of diversity which can be described as the point at which a service splits onto two bearers, each taking a different direction, and each being capable of taking the entire service, which is only achieved when the service functionality is allied with separation of service.

53. If the SPOF is vulnerable to sabotage the service provided by the SMS could be disrupted. Dutyholders should determine the potential impact of the consequences of malicious and non-malicious damage to SPOFs and consider arrangements to improve resilience by developing contingencies to operate around the loss of their functionality, design out the vulnerability, or harden the vulnerability with physical security controls.

8.8. Environmental Controls

54. SNI will be stored in a variety of locations and systems within dutyholder organisations and the environmental controls for all 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.

55. Environmental controls are often managed through Building Management System software and while that can be a pragmatic and cost-effective solution, inspectors should gain assurance that dutyholders have taken into account relevant factors such as any SPOF or vulnerabilities of sensors and remote management systems to assessed risks.

56. 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 ensure critical services are supported by a standby power supply or uninterruptible power supply solution in the event that the mains supply is disrupted. Other

essential services should be considered and addressed as per paragraphs 55-56.

Inspectors should consider

- Has a physical security plan been developed to describe the controls in place and is it appropriate?
- Is there a clear documented link between identified risks and the security controls in place?
- Has the purpose of physical security control measures been clearly defined and is the technical implementation adequate?
- Has the risk of overlooking and overhearing been considered in the siting of equipment used for processing SNI and meeting rooms where SNI is discussed?
- Is cable layout and security part of a planned and structured process?
- Has consideration been given to network patching security, the physical control of network ports in office areas and in data cabinets, and the implementation of controls around physical switch ports?
- Have TEMPEST/EMS considerations for the site been assessed and mitigated adequately where appropriate?
- What measures does the dutyholder have in place to limit the use of removable media devices?
- Is removable media being thoroughly scanned for malware before it is brought in to use or received from any other source?
- Does the dutyholder have a clear understanding of the risks around remote working? What physical and procedural security measures are in place to mitigate them adequately?
- Is there consideration to have a re-use and disposals policy in place, with key roles understood by everyone in your business?
- Are there records documenting the lifecycle of storage media and assets in terms of when they are in use and stored as well as the duration?
- How much physical storage space is available to store end-of-life equipment, and what are the security arrangements around storage and disposal?
- Have SPOFs been identified within the SMS infrastructure? What measures are in place to mitigate risks?

- Have any risks to the operation of environmental management systems been identified and mitigated adequately?
- Are ‘detect’ capabilities monitored appropriately?
- Has the dutyholder ensured that guard forces have clearly defined responsibilities and are SQEP for their roles? CNS-TAST-GD-9.3 [27] covers this topic in more detail.
- Is the dutyholder able to provide assurance that the alarm response force is trained and resourced adequately to respond to physical security events that affect SNI?

9. Assurance of Physical Security Measures

57. As with all security controls, assurance, and independent assurance, is required to ensure 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.

58. 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. CNS-TAST-GD-7.1 [13] describes the requirement for a risk management process managed by a security governance structure and physical security should be part of that approach.

59. 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 CNS-TAST-GD-1.1 [28] and CNS-TAST-GD-1.5 [29].

60. 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.

61. Dutyholders should have arrangements in place to ensure their security systems are subject to an appropriate regime of Examination, Inspection, Maintenance and Testing (EIMT) to ensure that they remain effective. Further guidance on these issues can be found in CNS-TAST-GD-5.2 [30].

9.1. Contractor Management

62. Dutyholders are responsible for managing risks to their information and associated assets held within their supply chain. Dutyholders should adopt a risk-based methodology to ensure that the level of assurance required for the physical protection of SNI is proportionate to the risk of loss, theft, unauthorised disclosure of, or unauthorised access to any SNI held either electronically or in physical (hard copy) form at a third-party premises. They should therefore approve the physical security (and other security) measures implemented by their contractors. This approval should take account of the requirements in GovS 007 [3], as qualified by the relevant FSyPs and RGP.

Inspectors should consider

- Is there adequate assurance that physical security measures are effective? Can they be scaled up as necessary?
- 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?
- Are all physical security measures adequately supported by procedural and personnel measures?
- Does the dutyholder ensure that SNI held within its supply chain is appropriately physically protected?
- Are supply chain facilities holding SNI suitably recorded and approved on List N?
- Does the duty holder have a suitable in contract monitoring process in place to ensure that security controls are maintained and remain commensurate to the risks they address, for the life of the contract or period that SNI will be held for?
- Does the dutyholder have arrangements in place to ensure their security systems are subject to an appropriate regime of EIMT?
- Is the dutyholder able to describe how they assure their physical security measures? List any supporting processes and procedures.

References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”.

[6] IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.

[7] IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011.

[8] IAEA, “Nuclear Security Series No. 23-G IAEA Implementing Guide: Security of Nuclear Information”.

[9] IAEA, “Nuclear Security Series No. 17 - Computer Security techniques for Nuclear Facilities”.

[10] ONR, “CNS-TAST-GD-7.2 - Information Security”.

[11] ISO, “ISO/IEC 27001:2013 - Information Technology”.

[12] IEC, “Understanding IEC 62443,” [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443.

[13] ONR, “CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management”.

[14] ONR, “CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations”.

[15] ONR, “CNS-TAST-GD-11.4.2 – The Threat”.

[16] CPNI, “Insider Risk Assessment,” [Online]. Available: https://www.cpni.gov.uk/insider-risk-assessment.

[17] CPNI, “CPNI Protective Security Risk Management,” [Online]. Available: https://www.cpni.gov.uk/rmm/protective-security-risk-management.

[18] CPNI, “CPNI Guide to Producing Operational Requirements for Security Measures,” [Online]. Available: https://www.cpni.gov.uk/system/files/documents/d5/76/Guide-to-producing-operational-requirements-for-security-measures.pdf.

[19] CPNI, “CPNI Asset Identification Guide,” July 2020. [Online]. Available: https://www.cpni.gov.uk/system/files/documents/2b/01/Asset%20Identification%20Guide%20v.2.pdf.

[20] CPNI, “CPNI Surreptitious Threat Mitigation Process v1,” 2021.

[21] NCSC, “NCSC TEMPEST and Electromagnetic Security,” [Online]. Available: https://www.ncsc.gov.uk/information/tempest-and-electromagnetic-security.

[22] NCSC, “NCSC Device Security Guidance,” [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-peripherals-securely.

[23] CPNI, “CPNI Remote and Overseas Working,” [Online]. Available: https://www.cpni.gov.uk/remote-and-overseas-working.

[24] NCSC, “NCSC Remote Working Advice & Guidance,” [Online]. Available: https://www.ncsc.gov.uk/section/advice-guidance/.

[25] NCSC, “NCSC Secure Sanitisation of Storage Media,” [Online]. Available: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

[26] CPNI, “CPNI Cyber Assurance of Physical Security Systems (CAPSS) – 2022 Security Characteristic,” February 2022. [Online]. Available: https://www.cpni.gov.uk/system/files/documents/fb/bc/capss-2022-security-characteristic-v10.pdf.

[27] ONR, “CNS-TAST-GD-9.3 - Security Guard Services”.

[28] ONR, “CNS-TAST-GD-1.1 - Security Governance and Leadership”.

[29] ONR, “CNS-TAST-GD-1.5 - Security Assurance Processes”.

[30] ONR, “CNS-TAST-GD-5.2 - Examination, Inspection, Maintenance and Testing (2019/135642)”.

[31] CPNI, “CPNI Catalogue of Security Equipment (CSE),” [Online]. Available: https://www.cpni.gov.uk/cse-categories.

[32] CPNI, “CPNI Guidance on the Control and Use of Key Locks,” [Online]. Available: https://www.cpni.gov.uk/system/files/documents/42/88/Guidance-on-the-control-and-use-of-key-locks.pdf.

[33] CPNI, “CPNI Guidance on the Control and Use of Combination Locks (CPNI Extranet)”.

Glossary and Abbreviations

AACS	Automatic Access Control System
CAPSS	Cyber Assurance of Physical Security Systems
CCTV	Closed Circuit Television
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
CSE	Catalogue of Security Equipment
EIMT	Examination, Inspection, Maintenance and Testing
EM	Electromagnetic
EMS	Electromagnetic Security
FSyP	Fundamental Security Principle
GovS 007	HMG Government Functional Standard 007: Security
HMG	Her Majesty’s Government
IAEA	International Atomic Energy Agency
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISF	Information Security Forum
ISO	International Organisation for Standardisation
IT/OT	Information Technology/Operational Technology
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
NIST	National Institute of Standards and Technology
NM	Nuclear Material
NSS	Nuclear Security Series
NTA	National Technical Authority
ONR	Office for Nuclear Regulation
OR	Operational Requirement
ORM	Other Radioactive Material
PIDS	Perimeter Intrusion Detection System
RGP	Relevant Good Practise
SMS	Security Management System

SNI	Sensitive Nuclear Information
SPOF	Single Point of Failure
SQEP	Suitably Qualified and Experienced Person
STaMP	Surreptitious Threat Mitigation Process
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
UK NACE	UK National Authority for Counter Eavesdropping
USB	Universal Serial Bus

Appendix 1: Types of Physical Security Control Measures

Physical security measures should be deployed in a defence in depth approach that provides layers to protect the information or information asset. The more effective layers of security controls that exist, the lower the probability of compromise of that data asset. The following control measures are broadly provided from the asset outwards, with their functions provided in line with CPNI guidance. Details of security furniture and equipment that meet the CPNI standard can be found in the CPNI Catalogue of Security Equipment (CSE) [31].

Table 1: Description of physical security control measures

Control Measure	Description
Envelope	To be an effective barrier an envelope should be used in conjunction with approved tamper seals to show evidence of compromise/attempted compromise.
Tamper Seal	Tamper seals provide physical evidence of unauthorised access when inspected and generate an appropriate response.
Container	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. They can provide an effective barrier to counter the threats from insiders, visitors and other personnel in the environment, particularly when supported by other security measures. Consideration should be given to adequately securing servers/workstations in approved lockable cabinets or containers where appropriate.

Control Measure	Description
Locking Mechanism	A lock and associated hardware must provide resistance against forcible attack techniques and/or those subtle methods associated with surreptitious attack. Key and Combination use and control procedures for the associated locking mechanism, should be applied in in line with RGP such as CPNI guidance [32] and [33].
Automated Access Control System (AACS)	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. 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. Consideration should be given to the identification and protection of its infrastructure during installation to provide assurance that the system cannot be compromised by an attacker.
Intrusion Detection System (IDS)	IDS should be considered for monitoring access to those rooms and areas and communications pathways, where information and associated assets may be stored or processed. IDS are intended to detect an unauthorised intrusion event and are only effective if used in concert with a response function (e.g., police, guard force or authorised users). Alarms should be of an approved type 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. 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. Consideration should be given to the identification and protection of its infrastructure during installation to provide assurance that the system cannot be compromised by an attacker.

Control Measure	Description
Secure Room	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, and they should be implemented as part of a single solution. Where secure rooms have been defined, the requirements for environmental management such as temperature control, ventilation and humidity should be taken into account. 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.
Door/portal	Security doors should be considered as a system comprising several components such as the door frame and fixings, supporting structure (cognisant of adjacent walls), and locking mechanism, and may be required to perform several functions such as control access, delay an adversary, emergency egress etc. They should show evidence of compromise or attempted compromise and be integrated with other security measures such as CCTV and IDS to be effective.

Control Measure	Description
Building/ Perimeter CCTV	A CCTV system must be capable of detecting attackers and their attack techniques. 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. 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 SQEP. CCTV systems may be subject to attack and dutyholders should consider potential vulnerabilities such as cables being compromised physically, cameras being obscured, remote control systems being taken over by hackers and signals intercepted and diverted elsewhere. 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 General Data Protection Regulations and the preservation of potential forensic evidence. Consideration should be given to the identification and protection of its infrastructure during installation to provide assurance that the system cannot be compromised by an attacker.
Visitors	Dutyholders should recognise the risk to sensitive assets posed by visitors. Lax practices and process failures may embolden malicious threat actors to attempt physical access to a site as part of a physical reconnaissance. An efficient and robust visitor reception regime, enforced by vigilant security/reception personnel, which incorporate stringent policies and procedures that are effectively implemented and understood by all staff and visitor hosts will act as a deterrent.

Control Measure	Description
Guarding	Many physical security measures rely upon human intervention to respond to alarms to prevent unauthorised access or damage to information and associated assets. Guard Force personnel (or other personnel performing equivalent functions) should have clearly defined responsibilities and procedures to deal with compromise and attempted compromise of controls protecting SNI and the capability to react effectively to associated alarms. They should be SQEP for their roles, especially 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.
Search	An effective search regime should detect, on both entry and exit to a site, devices capable of collecting or transmitting SNI and attempts to remove sensitive assets. It will also act as a deterrent if implemented effectively.
Fence	Fences and barriers, and integral gates, provide a limited delay to a determined intruder and to be effective should be supported by effective electronic surveillance detection capabilities such as CCTV and Perimeter Intrusion Detection System (PIDS) with an effective response function (e.g., police, guard force or authorised users). Security fencing often incorporates an overhang outward from the main fence to deter/delay intruders or can be topped with anti-scaling measures such as barbed tape coil.
Perimeter IDS (PIDS)	A number of factors should be considered when selecting a PIDS including the ground surface, local topography, prevailing weather conditions, and vicinity of conducting bodies. Defining the requirements of the system and ensuring a its effective commissioning will help achieve an appropriate detection rate. Consideration should be given to the identification and protection of its infrastructure during installation to provide assurance that the system cannot be compromised by an attacker.

Control Measure	Description
Security Lighting	Security lighting plays an important part in any site's security regime: providing a deterrence; increasing the uncertainty and vulnerability of an intruder during an intrusion; enabling detection and verification via CCTV; and will support a response force. However, whilst good quality and well-planned security lighting will fulfil several roles, to be effective and add value it must be considered as part of an integrated security solution.