Office for Nuclear Regulation

Security Assessment Principles for the Civil Nuclear Industry

2022 Edition, Version 1

Redgrave Court
Bootle
Merseyside
L20 7HS

Version Control

Development of the first Security Assessment Principles (SyAPs) was completed in March 2017 and is a product of extensive stakeholder engagement.

Changes may need to be made to this document as time moves on, for example amending minor typing errors, or accommodating any significant changes affecting the Office for Nuclear Regulation (ONR).

For this reason the website version is the only authorised version.

To avoid any confusion and provide some form of version control over the guidance, every page in this paper copy is marked as 'uncontrolled if not viewed on ONR website'. This signals that at a future date the information may change, and it is the responsibility of each individual to cross reference any copy with the most up to date version published on the ONR website.

Where amendments are made to the document, these will be published on the ONR website with an audit trail and, where possible, stakeholders will be alerted to the changes.

Revision History

No.	Date	Change summary
0	31 March 2017	Original Issue
1	31 March 2022	Publication of Version 1

FOREWORD

The Office for Nuclear Regulation (ONR) is the independent regulator of nuclear safety and civil nuclear security across the UK. ONR use these Security Assessment Principles (SyAPs), together with supporting Technical Assessment Guides (TAGs), to guide regulatory judgements and recommendations when undertaking assessments of dutyholders' security submissions such as site security plans and transport security statements. Underpinning the requirement for these submissions, and ONR's role in their approval, are the legal duties placed on organisations subject to the Nuclear Industries Security Regulations (NISR) 2003.

The SyAPs provide the essential foundation for the introduction of outcome focussed regulation for all constituent security disciplines: physical; personnel; transport; and cyber security and information assurance. This regulatory philosophy is aligned with our mature non-prescriptive nuclear safety regime and provides dutyholders with a coherent regulatory approach applied by ONR across the UK civil nuclear industry. Introduction of SyAPs represents a pivotal shift away from prescription which has been made possible by the significant improvements in security management capability and capacity developed within dutyholder organisations since the establishment of formal regulation under NISR 2003.

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

This is the first issue of the SyAPs and it is expected to take time to embed and reach full maturity. Implementation at this juncture is particularly beneficial given the diverse nature of the industry that includes new build design and construction, power operations, and extensive decommissioning. The approach enables the dynamic nature of the threat to be accounted for and proactively responded to by the dutyholders. ONR recognises that learning from the new approach and the evolving threat, notably in the cyber area, may require the SyAPs to be refined during this implementation phase, a review is planned after 12 months.

The UK is a signatory to the United Nations International Convention for the Suppression of Acts of Nuclear Terrorism and is therefore obliged to make every effort to adopt appropriate measures to ensure the protection of radioactive material, taking into account relevant recommendations and functions of the International Atomic Energy Agency. The UK is also a signatory to the International Atomic Energy Agency Convention on the Physical Protection of Nuclear Material (CPPNM). The CPPNM places

obligations on signatory states to protect nuclear facilities and material in peaceful domestic use and storage as well as in transit. Fundamental principles within the CPPNM oblige signatory states to establish a legislative and regulatory framework to govern physical protection; and an independent, competent authority with adequate resources to implement that framework. ONR is this independent competent authority in the UK and SyAPs form part of the regulatory framework.

The Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) have supported ONR in the development of SyAPs and their contribution is gratefully acknowledged.

This first issue of SyAPs has been informed and developed with extensive stakeholder engagement including a diverse range of industry dutyholders, the Nuclear Decommissioning Authority and the Department for Business, Energy and Industrial Strategy. Additional stakeholders who have reviewed the SyAPs during their development include the Chief Nuclear Inspectors' Independent Advisory Panel, the Safety Directors Forum security sub-group and the IAEA International Physical Protection Advisory Service mission to the UK in 2016. Comments and views submitted to us during consultation have, in many cases led us to modify the text. However, decisions on the final text and responsibility for the SyAPs content are ours alone.

Chief Nuclear Inspector
Office for Nuclear Regulation

31 March 2017

1 INTRODUCTION

1.1 UNIFYING PURPOSE STATEMENT

Unifying Purpose Statement	UPS
Civil Nuclear Industry dutyholders (hereafter 'dutyholders') are responsible for the leadership, design, implementation, operation and maintenance of security arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of Nuclear Material (NM)/Other Radioactive Material (ORM) and supporting systems or through the compromise of Sensitive Nuclear Information (SNI).	

1. The State retains responsibility for the maintenance of the legislative and regulatory framework within which dutyholders discharge their security responsibilities. Dutyholders should integrate their security responsibilities with those for safety and nuclear materials safeguards. These security responsibilities are implemented using a graded, risk-managed approach instructed by an assessment of the threat, that builds defence in depth and expects continuous review and improvement.

1.2 THE PURPOSE OF THE SECURITY ASSESSMENT PRINCIPLES

2. The Security Assessment Principles (SyAPs) apply to assessments of security arrangements defined in security plans as well as the control of Sensitive Nuclear Information (SNI) held on and off nuclear facilities. The term 'security plan' is used throughout this document to encompass the totality of the documentation produced by a developer, licensee or other dutyholder to demonstrate high standards of nuclear security. This includes, for example, site security plans, transport security plans, Transport Security Statements (TSSs) and temporary security plans and any subset of this documentation that is submitted to the Office for Nuclear Regulation (ONR).

3. The principles presented in this document relate only to civil nuclear security. Non-nuclear related security is excluded. NM and facilities used primarily for defence purposes are also excluded. The use of the word 'security' within the document should therefore be interpreted accordingly.

4. The primary purpose of the SyAPs is to provide ONR with a framework for making consistent regulatory judgements on the adequacy of security arrangements. The principles are supported by Technical Assessment Guides (TAGs), and other guidance, to further assist decision making within the nuclear security regulatory assessment process. Although it is not their primary purpose, the SyAPs may also provide guidance to designers and dutyholders on the appropriate content of security plans, clarifying our expectations in this regard. However, they are not sufficient on their own to be used as design or operational standards, nor are they intended for that purpose.

1.3 REGULATORY BACKGROUND

5. Part 3, Chapter 1 of The Energy Act (TEA) 2013 (Reference 1) defines ONR's purposes thus:

    (a) Nuclear Safety;

    (b) Nuclear Site Health and Safety

    (c) Nuclear Security;

(d) Nuclear Materials Safeguards; and,

(e) Transport (of radioactive material).

6. For the purposes of TEA, Relevant Statutory Provisions (RSPs) are:

(a) Part 3 of TEA

(b) Nuclear Regulations (including The Nuclear Industries Security Regulations (NISR) (Reference 2) and 'Class 7' aspects of the Carriage of Dangerous Goods & Use of Transportable Pressure Equipment Regulations)(Reference 3);

(c) Sections 1, 3-6, 22 & 24A of the Nuclear Installations Act 1965 (Reference 4); and,

(d) The Nuclear Safeguards Act 2000 (Reference 5).

7. In accordance with the RSPs above, ONR regulates the security of civil nuclear premises[1], the security of the transport of Category I – III Civil NM within Great Britain or internationally by UK flagged vessels, and the security of SNI wherever it is held within the UK. It also regulates nuclear safety on nuclear licensed sites and facilitates UKs international civil nuclear materials safeguards obligations.

8. Our role in regulating civil nuclear security includes approving security plans, inspecting compliance with arrangements made under these plans, exercising other controls and making judgements on the acceptability of responses made by dutyholders to the requirements placed on them by NISR. Though ONR regulates civil nuclear security, it is also the Vetting Authority for the civil nuclear industry, required to follow processes that achieve the Baseline Personnel Security Standard and National Security Vetting as mandated by HM Government.

1.4 PERMISSIONING

9. Within the nuclear industry, regulatory regimes requiring security submissions and/or a licence are referred to as 'permissioning regimes'. ONR's approach to such regimes is set out in the ONR document titled 'Purpose and Scope of Permissioning' (Reference 6). Most security submissions to ONR arise from NISR requirements (for example site security plans and TSSs for approval), but some also support Generic Design Assessment (GDA).

1.5 INTERFACE WITH OTHER REGULATORY BODIES

10. Depending on the nature of the security plan being assessed, there may be other regulators whose requirements and processes ONR needs to take into account when coming to a regulatory decision. These interactions are covered by relevant joint statements, memoranda of understanding and other agreements.

1.6 INTERNATIONAL FRAMEWORK AND CONTEXT

1.6.1 Responsibilities of the State

11. The UK is a member state of the International Atomic Energy Agency (IAEA) and a signatory to the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 7) and its amendment (Reference 8). Accordingly, the UK recognises its

[1] Nuclear Premises as defined by NISR 2003 Regulation 2

responsibility for establishing, implementing and maintaining a physical protection regime effective against theft and sabotage for all civil nuclear facilities, civil NM in use/process, storage, and during transport; and protection of technology and SNI against compromise. Furthermore, these responsibilities extend to ensuring that civil NM is adequately protected during international transport on UK flagged vessels, until that responsibility is transferred to another state.

1.6.2 Legislative and Regulatory Framework

12. The UK is obliged to establish and maintain a legislative framework to govern physical protection of NM, ORM and SNI. The framework should provide for the application of physical protection requirements and include a system of evaluation, permissioning and compliance inspection, together with a means of enforcement, including effective sanctions.

13. The framework for the regulation of civil nuclear security within the UK consists principally of TEA 2013 and NISR 2003. The latter establishes the system of approvals and reporting. It also allows directions to be made and specifies offences, thus providing effective tools of enforcement and sanction.

1.6.3 Competent Security Authority

14. In order to ensure that the legislative and regulatory framework is implemented effectively, states are required to establish a competent authority responsible for regulation. Part 3 of TEA sets out the provisions which establish ONR as a statutory body, describes its purposes (one of which is nuclear security) and establishes its powers. NISR 2003 is a RSP of TEA, which ONR is empowered to enforce as the competent authority. Regulations have also been made under the TEA (in particular, the Nuclear Industries Security (fees) Regulations (Reference 9)) that require fees to be paid for the performance of any function by or on behalf of the Secretary of State in connection with putting into effect the principal Regulations. Under these arrangements ONR is also the Vetting Authority for the civil nuclear industry.

15. Together, TEA, NISR and other relevant statutory provisions ensure that ONR has sufficient authority, independence (from organisations involved in the promotion of utilisation of nuclear energy) and financial/human resources available to fulfil its responsibilities of regulating civil nuclear security. The diagram below shows how ONR inspectors are empowered to enforce NISR through TEA.

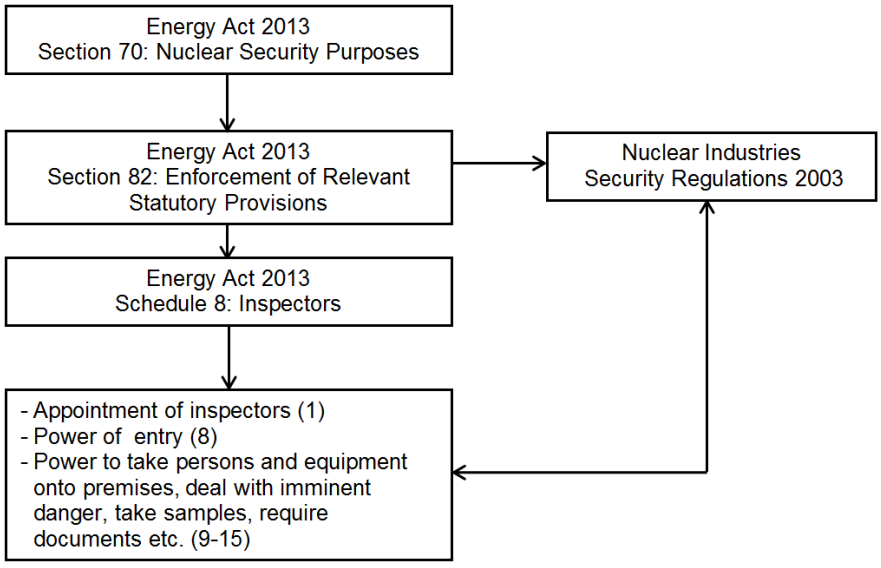

Figure 1 – Civil Nuclear Security Regulatory Legislation

16. Whilst ONR's focus is on UK civil nuclear security regulation, it contributes actively to the development of the Nuclear Security Series (NSS) documents published by the IAEA. Through ONR, the UK applies these international security standards and ensures that its own regulations, regulatory requirements and guidance are consistent with them. These SyAPs are part of regulatory guidance, which, together with TEA and NISR assist the UK regime to comply with its obligations under CPPNM.

17. In addition to working with IAEA on the NSS, ONR assists Her Majesty's Government on matters arising from IAEA security work and meetings. ONR's guidance to inspectors seeks to take account of developing advice and guidance arising from the work of all these and other relevant organisations.

1.6.4 Responsibilities of Dutyholders

18. NISR clearly identifies responsible persons, approved carriers and relevant personnel (which may include officers, employees and contractors to whom Regulation 22 applies) and places requirements on them. This ensures that prime responsibility for the implementation of arrangements for protection of NM, ORM, and associated facilities and SNI rests with the dutyholders.

19. Within this document, the generic term dutyholder is used to describe 'a responsible person', 'approved carriers' and 'relevant personnel' as defined in NISR.

1.7 APPLICATION OF THE SYAPS

1.7.1 General

20. The SyAPs contain principles and guidance. The principles form the underlying basis for regulatory judgements made by inspectors, and the guidance associated with the principles provides either further explanation of a principle, or their interpretation in actual applications and the measures against which judgements can be made.

21. The principles are a reference set from which the inspector should select those relevant to the particular situation. Not all of the principles in this document apply to all assessments or every dutyholder; principles specific to nuclear premises may not apply to a location which holds only SNI. Less obviously, not all of the security principles apply to all nuclear premises, such as those specific to construction sites, adjacent facilities or where the Civil Nuclear Constabulary (CNC) are deployed. Additionally, the assessment of a temporary security plan or arrangement will only require the relevant principles to be applied.

22. The regulation of security arrangements for any nuclear premises controlled or operated wholly or mainly for the purposes of the department of the Secretary of State with responsibility for defence does not fall within ONR's responsibilities. Neither does the regulation of security for non-civil licensed nuclear sites/facilities holding Category IV quantities of nuclear material or radioactive sources. The latter is the responsibility of the Environment Agency, the Scottish Environment Protection Agency or Natural Resources Wales, with advice provided by Counter-Terrorism Security Advisors. However, ONR maintains regular liaison with these organisations to ensure consistent protective security approaches are adopted.

1.7.2 Relationship to National Policy Documents

23. NISR places a legal requirement to protect SNI. Some dutyholders are also government organisations and are therefore required to protect sensitive information (including SNI) in accordance with the HMG publication Government Functional Standard GovS 007: Security (hereafter termed GovS 007) (Reference 10) produced by the Government Security Group (reference 10). This document 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 GovS 007 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. Therefore, security plans submitted to ONR for approval (or prepared to demonstrate compliance with Regulation 22) that address these principles may be adequate to fulfil obligations to protect SNI as required by both NISR and GovS 007.

24. The Cabinet Office sets minimum standards to be met to achieve a Baseline Personnel Security Standard (BPSS) and/or National Security Vetting (NSV) clearance, therefore arrangements in this regard are prescriptive HMG expectations for personnel Security are described in the 'Cabinet Office SPF Personnel Security Supplement' and 'HMG Baseline Personnel Security Standard Guidance on the Pre-employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors'. Both of these documents are identified as relevant good practice. They describe the Cabinet Office 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. ONR is nominated as the vetting authority for the civil nuclear industry. In its capacity as the decision maker on the suitability of individuals to hold a National Security Vetting clearance, ONR may require information beyond that articulated in HMG guidance in order to take vetting decisions. Such information is non-discretionary and is not subject to interpretation under SyAPs arrangements.

1.7.3 Lifecycle

25. The SyAPs are designed to support regulatory assessments throughout the lifecycle of nuclear facilities. Specific sections are, however, devoted to individual stages, e.g. construction. In general, not every principle in every section will apply to every lifecycle stage. Instead the principles are a reference set from which the inspector should select those relevant to the particular stage in the lifecycle. For instance, the sections on Leadership and Management for Security and the Regulatory Assessment of Security Plans include aspects covering the entire lifecycle of the facility. The SyAPs are relevant to design, construction, manufacture and installation, but will also apply to later operational stages. Commissioning is a key stage in providing the necessary assurance of security and a number of the principles include aspects of commissioning. Decommissioning should also be considered at all lifecycle stages.

1.7.4 New Facilities

26. SyAPs support the regulatory security assessment of new (proposed) nuclear facilities. They represent ONR's view of good practice and we would expect modern facilities to satisfy their overall intent.

1.7.5 Facilities Built to Earlier Standards

27. Inspectors should assess security plans against the relevant SyAPs when judging if a dutyholder has demonstrated that legal requirements and regulatory security outcomes have been met and risks have been proportionately managed and mitigated. The extent to which the principles ought to be satisfied must also take into account the age of the facility or plant. For facilities designed and constructed to earlier standards, the issue of whether suitable and sufficient compensatory security measures have been implemented will need to be judged plan by plan.

1.7.6 Transient Risks

28. For certain activities, such as decommissioning, it is recognised that some principles may not be met transiently. This may be allowable provided the result is to achieve an equal or more secure end-state. However, this period should be minimised and the requirement to reduce risks remains.

1.7.7 Ageing

29. As a facility ages, some security measures may become degraded and dutyholders may argue that making improvements is not cost effective. The short remaining lifetime of the facility may be invoked as part of the security plan demonstration. However, this factor should not be accepted to justify the facility not achieving a proportionate security outcome or maintaining an appropriate posture and compensatory security measures may be required.

30. A security plan which argues for not making an improvement based predominantly on limited future lifetime should only be accepted where the maximum extent of the future operational life is irrevocably fixed and provides a suitable level of security. In cases where the risks mitigated by the security plan will remain in place for typically greater than 5 years, adequate sustainable arrangements will need to be demonstrated to manage these on-going risks.

1.7.8 Continuous Improvement and Annual Security Reviews

31. The principle of continuous improvement is central to achieving sustained high standards of nuclear security. Adversaries may seek to enhance their capabilities to defeat security technologies. Application of this principle ensures that, no matter how high the standards of nuclear security design and subsequent operations, further improvements should always be considered. Seeking and applying lessons learned from events, new knowledge and experience, both nationally and internationally, should be a fundamental feature of the security culture of the nuclear industry.

32. The SyAPs also provide a framework that can be applied during annual reviews of security that assess performance and efficacy of the security plan. These annual reviews should be supplemented with more comprehensive reviews at an appropriate frequency.

1.7.9 Safety and Security Assessments

33. Safety and security legislation imposes separate, specific duties on licensees and dutyholders. Sometimes these duties are inter-related. For instance, while malicious acts such as theft or sabotage would not normally be considered when determining the reasonably practicable preventative or protective measures needed in the interests of safety, what might be done to mitigate the consequences from such acts should nevertheless be considered within safety and security assessments.

34. The aims of safety and security legislation are complementary; in that both are intended to lead to measures that reduce the risk of harm to the public and workers arising from nuclear facilities, and so measures that adequately address the requirements of one set of legislation may satisfy the requirements of the other. On other occasions a common solution will not be possible, and designers or dutyholders will need to determine a solution that separately addresses the requirements of safety and security legislation. In practical terms this may mean (for instance to reduce the total amount of documentation required) that designers or dutyholders may choose to combine safety and security-derived assessments into single documents, or choose to keep those parts of the security plan which are also needed to meet safety duties separate from the rest of the security plan. Such approaches are perfectly acceptable provided the totality of these documents addresses all of ONR's expectations and requirements in the two areas. In particular, the combining of assessments in this way should not be taken to imply that security assessments lie within the remit of safety legislation, or vice versa.

35. Given this complementary relationship between safety and security, these SyAPs also include guidance on how to assess safety-related matters where these fall within the vires of security legislation, e.g. because of overlap or inter-relation. This guidance is provided in the specific sections of the principles where this applies. Detailed information on safety aspects can be found in the Safety Assessment Principles 2014 document (Reference 12).

1.7.10 Multi-Facility Sites

36. When considering the security threats to a nuclear site, every facility, service and activity on a site must be included. In some plans, the SyAPs may be applied in relation to single facilities and so the control of risks can be considered on a facility basis. However, there is also a need to consider the totality of risks from a site perspective and how these are controlled (for example when a single initiating event can affect multiple facilities). In some locations there are multiple sites, governed by different dutyholders, e.g. where there are neighbouring sites or tenants. In this circumstance, ONR expects dutyholders to co-operate with one another so that the threats in the location, taking into account all neighbouring sites, are mitigated.

37. Individual sites with multiple facilities may produce individual security plans for each facility and larger sites may benefit from adopting a modular approach. Shared services may also generally be dealt with by separate plans. The division of a site's security plan in this way requires the definition of boundaries and interfaces between facilities, facilities and services, and services. It also requires an appropriate combination of the individual assessments to provide an overall security plan which accounts for the interactions and interdependencies between facilities and services.

1.7.11 Alternative Approaches

38. The SyAPs express ONR's expectations for the content of security plans submitted to us. However, designers and/or dutyholders may wish to put forward security plans that differ from these expectations. ONR inspectors should consider such submissions on their individual merits. That said, where the approach being followed differs substantially from the expectations set out here, designers and/or dutyholders may wish to discuss the method of demonstration with ONR beforehand. ONR will need to be assured that such plans demonstrate equivalence to the outcomes associated with the use of the principles here and such a demonstration may need to be examined in greater depth to gain that assurance.

1.8 STRUCTURE OF THE PRINCIPLES

39. This section (1) defines the unifying purpose for dutyholders' security regimes and provides context (including international aspects) to the SyAPs. Section 2 contains the Fundamental Security Principles (FSyPs). These principles are founded in UK security law and/or international good practice, and underpin all activities that contribute to sustained high standards of nuclear security. They fall into two categories:

    (a) Strategic Enablers – FSyPs 1-5 are focussed on creation of the right conditions to support high reliability security arrangements; and,

    (b) Secure Operations – FSyPs 6-10 are focused on the implementation and maintenance of nuclear security.

40. Each FSyP is supported by one or more Security Delivery Principle (SyDP), as detailed in Section 3. Notwithstanding alternative approaches detailed above, it is against these principles that inspectors judge the adequacy of a dutyholder's submission.

41. Section 4 contains Key Security Plan Principles (KSyPPs), which should be applied across the breadth of the FSyPs and SyDPs covered in any security plan submitted to ONR for approval.

42. NISR 2003 requires that certain security plans such as site security plans and TSSs are approved by ONR. Section 5 is concerned with the regulatory assessment of security plans and provides guidance that sets the foundation for the production and assessment of right first time, effective security plans. It is underpinned by the concepts and principles articulated within the Regulatory Assessment of Security Plans (RASyP).

43. The glossary at the end of the principles is provided to assist in understanding some of the terms used. Where relevant, the glossary includes the sources of the definitions adopted. Abbreviations and references are also provided to assist readers' understanding.

44. This document has been developed following the regulators code, particularly regarding engagement with those we regulate and ensuring that our approach to regulatory activities is transparent and easily accessible, including being available at a single point on our website. However, certain elements of the framework are SNI and require appropriate control. In order to allow publication of SyAPs, these elements have been compartmentalised within a suite of annexes, which will be made available to those with a demonstrable need to know and the required means to ensure protection.

45. The diagrams below show the relationship between the different sections of the document and how they relate to the assessment of security plans and NISR 2003 Regulation 22 compliance for those holding SNI.

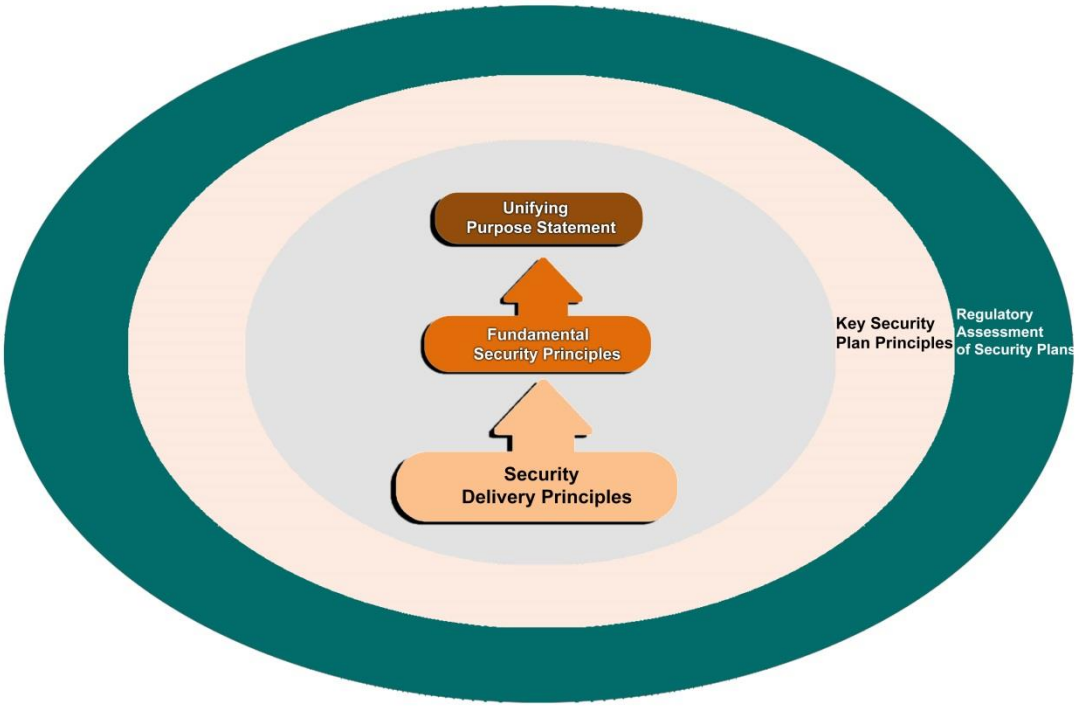

Figure 2 – Structure of the Security Assessment Principles

THIS PAGE IS INTENTIONALLY BLANK

Fundamental Security Principles

1 - Leadership and Management for Security
2 - Organisational Culture
3 - Management of Human Performance
4 - Nuclear Supply Chain Management
5 - Reliability, Resilience and Sustainability
6 - Physical Protection Systems
7 - Cyber Security and Information Assurance
8 - Workforce Trustworthiness
9 - Policing and Guarding
10 - Emergency Preparedness and Response

Security Delivery Principles

1.1 - Governance and Leadership
1.2 - Capable Organisation
1.3 - Decision Making
1.4 - Organisational Learning
1.5 - Assurance Processes

2.1 - Maintenance of a Robust Security Culture

3.1 - Identification and Analysis of Security Tasks and Roles
3.2 - Sufficiency and Competence of Personnel Delivering Security
3.3 - Suitable and Sufficient Workspaces, Equipment and User Interfaces
3.4 - Suitable and Sufficient Procedures and Administrative Controls

4.1 - Procurement and Intelligent Customer
4.2 - Supplier Capability
4.3 - Oversight of Suppliers of Items or Services that may Impact on Nuclear Security
4.4 - Commissioning

5.1 - Reliability and Resilience
5.2 - Examination, Inspection, Maintenance and Testing
5.3 - Sustainability

6.1 - Categorisation for Theft
6.2 - Categorisation for Sabotage
6.3 - Physical Protection System Design
6.4 - Vulnerability Assessments
6.5 - Adjacent or Enclave Nuclear Premises
6.6 - Nuclear Construction Sites
6.7 - Protection of Nuclear Material During Offsite Transportation

7.1 - Effective Cyber and Information Risk Management
7.2 - Protection of Information
7.3 - Protection of Nuclear Technology and Operations
7.4 - Physical Protection of Information
7.5 - Preparation for and Response to Cyber Security Incidents

8.1 - Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security
8.2 - Pre-employment Screening and National Security Vetting
8.3 - Ongoing Personnel Security

9.1 - CNC Response Force
9.2 - Local Police Operations in Support of the Dutyholder
9.3 - Security Guard Services

10.1 - Counter Terrorism Measures, Emergency Preparedness and Response Planning
10.2 - Testing and Exercising the Security Response
10.3 - Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event

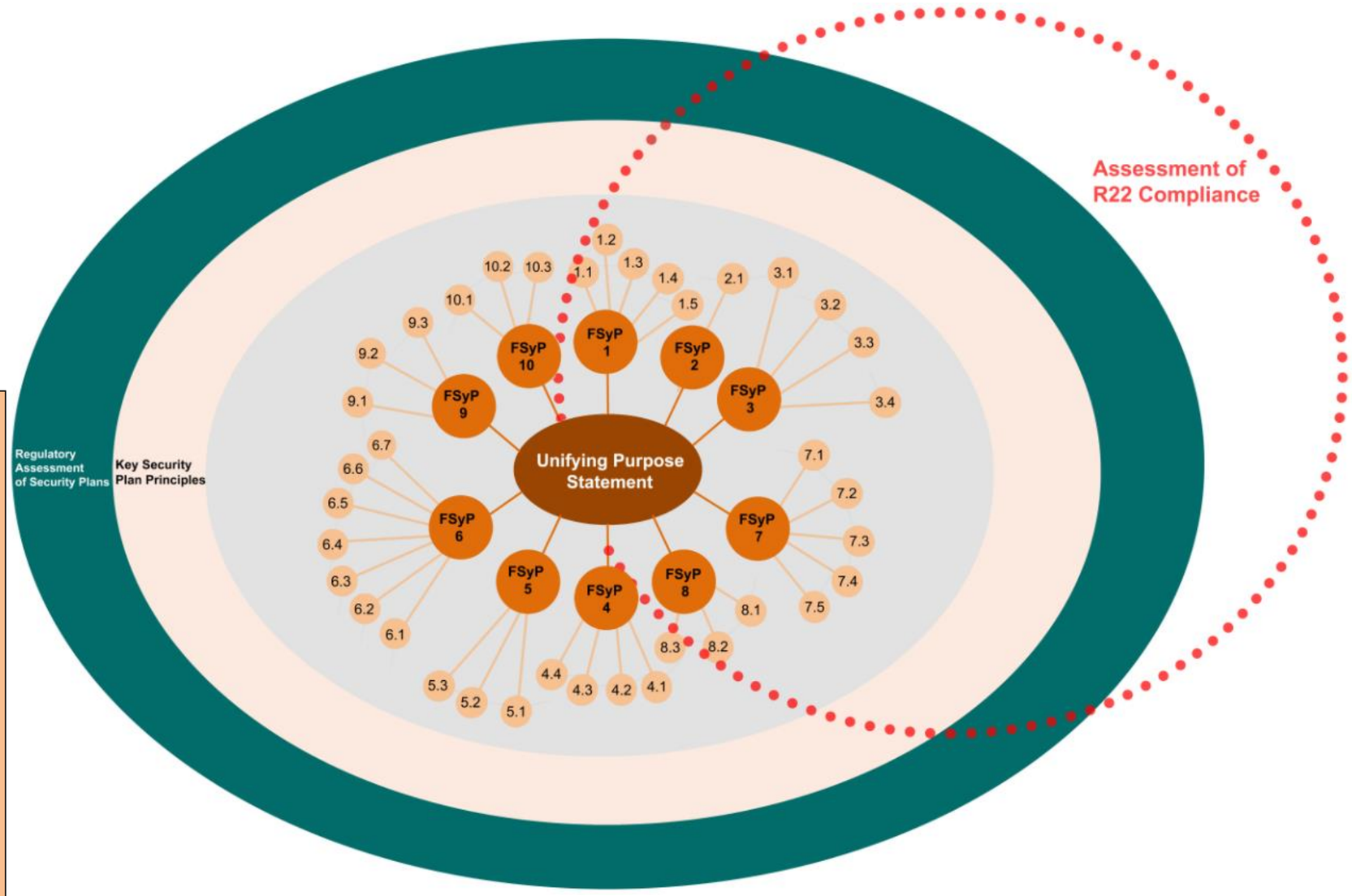

Figure 3 – Detailed Structure of the Security Assessment Principles as Applied to Assessments of Security Plans and Compliance with Regulation 22 of NISR 2003

THIS PAGE IS INTENTIONALLY BLANK

2 FUNDAMENTAL SECURITY PRINCIPLES

46. The fundamental security principles are considered to be the foundation for the subsequent security delivery principles in this document. They reflect UK law, obligations under the CPPNM and accepted international good practice in the IAEA NSS, in particular the Fundamentals detailed in No. 20 'Objective and Essential Elements of a State's Nuclear Security Regime' and the Recommendations detailed in No. 13 'Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities' and No 14. 'Nuclear Security Recommendations on Radioactive Material and Associated Facilities'; and in recognition of their legal standing, use the 'must' form rather than 'should'.

47. The CPPNM and IAEA NSS also include Fundamentals and Recomendations which are not related to assessment. These include aspects such as responsibilities of the State, the establishment of a legislative and regulatory framework and a competent authority. The UK's approach to these aspects is provided in the introductory section above. The fundamental security principles have therefore been drawn from the aspects of CPPNM and the IAEA NSS that are relevant to the remit of the SyAPs for the assessment of dutyholder submissions under the requirements of NISR 2003.

2.1 FSYP 1 - LEADERSHIP AND MANAGEMENT FOR SECURITY

Fundamental Security Principles	Leadership and Management for Security	FSyP 1
Dutyholders must implement and maintain organisational security capability underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.		

2.2 FSYP 2 - ORGANISATIONAL CULTURE

Fundamental Security Principles	Organisational Culture	FSyP 2
Dutyholders must encourage and embed an organisational culture that recognises and promotes the importance of security.		

2.3 FSYP 3 - MANAGEMENT OF HUMAN PERFORMANCE

Fundamental Security Principles	Management of Human Performance	FSyP 3
Dutyholders must implement and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately designed (to include tasks, competent staffing, workspaces, equipment and administrative control), implemented and resourced.		

2.4 FSYP 4 - NUCLEAR SUPPLY CHAIN MANAGEMENT

Fundamental Security Principles	Nuclear Supply Chain Management	FSyP 4
Dutyholders must implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security.		

2.5 FSYP 5 - RELIABILITY, RESILIENCE AND SUSTAINABILITY

Fundamental Security Principles	Reliability, Resilience and Sustainability	FSyP 5
Dutyholders must design and support their nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle.		

2.6 FSYP 6 - PHYSICAL PROTECTION SYSTEMS

Fundamental Security Principles	Physical Protection Systems	FSyP 6
Dutyholders must implement and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack.		

2.7 FSYP 7 - CYBER SECURITY AND INFORMATION ASSURANCE

Fundamental Security Principles	Cyber Security & Information Assurance	FSyP 7
Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.		

2.8 FSYP 8 - WORKFORCE TRUSTWORTHINESS

Fundamental Security Principles	Workforce Trustworthiness	FSyP 8
Dutyholders must implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.		

2.9 FSYP 9 - POLICING AND GUARDING

Fundamental Security Principles	Policing and Guarding	FSyP 9
Dutyholders must demonstrate effective guarding and policing arrangements, integrating the operations of relevant police forces (e.g. CNC, BTP) and security guard services.		

2.10 FSYP 10 - EMERGENCY PREPAREDNESS AND RESPONSE

Fundamental Security Principles	Emergency Preparedness and Response	FSyP 10
Dutyholders must implement and maintain effective security Emergency Preparedness and Response arrangements which are integrated with the wider safety arrangements.		

THIS PAGE IS INTENTIONALLY BLANK

3 SECURITY DELIVERY PRINCIPLES

48. These principles comprise specific outcomes focused on the delivery of an effective nuclear security regime that dutyholders must demonstrate that they have addressed within their security plan. The wording in italic font is intended to provide further context to the discipline being covered by the FSyP to which the subsequent SyDPs relate and is included for information only. As such, it does not contain any regulatory expectations, which are articulated by the SyDPs and associated qualifiying text.

49. As indicated above, the SyDPs are directly linked to the FSyPs. Accordingly, principles linked to FSyPs 1-5 are concerned with enabling the delivery of effective security strategy, whilst those linked to FSyPs 6-10 are concerned with the delivery of secure operations.

50. The SyDPs relating to FSyPs 1, 2, 3, 7 & 8 incorporate relevant content from GovS: 007 for the protection of information and to achieve mandated pre-employment control and national security vetting requirements. They apply equally to both nuclear premises, approved carriers and non-nuclear locations that hold SNI and will therefore be used by ONR as a basis to form judgements as to the effectiveness of Cyber Security and Information Assurance (CS&IA) and Workforce Trustworthiness arrangements for all dutyholders.

3.1 FSYP 1 - LEADERSHIP AND MANAGEMENT FOR SECURITY

Fundamental Security Principle	**Leadership and Management for Security**	**FSyP 1**
Dutyholders must establish and maintain organisational security capability underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.		

51. The principles in this section enable the effective delivery of nuclear security. Inspectors should use these principles proportionately, reflecting the categorisation for theft and sabotage and the scale and complexity of the dutyholder's undertaking.

52. This fundamental principle contains five high-level inter-related principles: Governance & Leadership, Capable Organisation, Decision Making, Learning and Assurance. These set the outcomes to be achieved for effective leadership and management for security, rather than describing the systems, processes and procedures for achieving security. Because of their inter-connected nature there is some overlap between the principles. Therefore it is necessary for them to be considered as a whole and delivered via an integrated approach.

53. The principles combine the key features of effective security management arising from current national law and guidance (in particular NISR 2003 and TEA). They also draw on international guidance including IAEA security standards and relevant good practice in security management.

54. In combining the key features of leadership and management for security from a range of sources, the principles reflect:

    (a) the emphasis ONR gives to leadership and management for security, the role of the Board, directors and worker involvement;

(b) the pivotal role played by good and effective leadership, people management and processes; and

(c) the need to consider the management of security at all levels throughout the whole organisation in building and sustaining a positive security culture.

3.1.1 SyDP 1.1 - Governance and Leadership

FSyP 1 - Leadership and Management for Security	Governance and Leadership	SyDP 1.1
Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of security and on delivering the characteristics of a high reliability organisation.		

55. Robust governance includes clear terms of reference to ensure a coherent, direct chain of accountability for security through to the main board member responsible for security oversight. Reporting structures should be clearly understood, with well-defined budget responsibilities and delegated personal authorities.

56. Leadership is key to achieving appropriate, high levels of security and establishing and sustaining a positive security culture. In meeting Principle SyDP 1.1 the expectation is that the behaviour and activities of directors, managers and other leaders should include:

(a) establishing the strategies, policies, plans, goals and standards for security and ensuring that they are delivered throughout the organisation;

(b) providing direction, governance and oversight to establish and foster an organisational culture that underpins secure operations;

(c) demonstrating a visible commitment to security through their activities;

(d) recognising and resolving conflict between security and other goals (e.g. safety, production and commercial pressures);

(e) ensuring that security is participative, actively drawing on the knowledge and experience of all staff;

(f) ensuring that performance management tools promote the identification and management of risk, encourage positive security behaviours and discourage insecure, risky behaviours or complacency;

(g) understanding that apparent past success is no guarantee of future success and that fresh perspectives on ways to enhance security should be sought and acted upon; and

(h) monitoring and regularly reviewing security performance and culture.

57. The value of security as an integral part of good business and management practice should be reinforced through interactions between directors, managers, other leaders and staff, including contractors, to establish a common purpose and collective organisational responsibility. Consultation and involvement of all staff secures effective engagement and co-operation in the development, maintenance and improvement of security and promotes a shared concern for achieving security goals.

As a result, people at all levels in the organisation should be engaged in a common purpose that recognises responsibility and accountability to each other and external stakeholders to ensure high standards of security. The dutyholder should ensure that this extends to contractors down the supply chain as required.

58. Oversight of security performance, led by the board of the organisation, should provide assurance at all levels, and throughout all stages of the life of the undertaking, that security is being maintained and improved. It should utilise diverse sources of information, including feedback from independent challenge and reviews, in order to provide confidence (by means of governance, monitoring and auditing processes) that security and quality policies, strategies, plans, goals, standards, systems and procedures are being implemented through the application of an effective management system.

59. The management system should give due regard to security, and security should be considered explicitly when developing and implementing any new arrangements for managing the organisation. An integrated management system should be adopted so that the potential for conflicts between the organisation's goals and responsibilities is minimised. The management system should:

(a) be based on national or international standards or equivalent;

(b) be aligned with the goals of the organisation and contribute to their achievement;

(c) be subject to regular review, seeking continual improvement; and

(d) support a positive security culture.

3.1.2 SyDP 1.2 - Capable Organisation

FSyP 1 - Leadership and Management for Security	Capable organisation	SyDP 1.2
The organisation should have the capability to implement and maintain the security of its undertakings.		

60. The organisation should have adequate Human Resources (HR), including occupational health capability. This includes having the necessary competencies, experience and knowledge in sufficient numbers to provide resilience and maintain the capability to govern, lead and manage security at all times. A properly resourced security governance structure should typically include (but is not limited to) the following roles:

- Board member responsible for security
- Director or Chief Security Officer
- Internal Regulator/Assurance
- Senior Information Risk Officer
- Departmental Security Officer
- Information Asset Owner
- Chief Information Security Officer
- Other information risk assessment and risk management specialists

- Other specialists relevant and specific to the organisation's needs

61. In addition an individual who is responsible for nuclear security with sufficient authority, autonomy and resources to implement and oversee all nuclear security activities should be appointed. The organisation's structure and baseline staffing levels should be based on appropriate organisational design principles. HR baseline provisions should be established, controlled and reviewed regularly through robust, auditable processes. Changes to the organisation (including to structure, staffing, resources or competencies) should be subject to systematic evaluation to ensure that they do not adversely affect the capability of the organisation to deliver security. There should be succession planning arrangements (especially where there is limited or singleton expertise). Succession planning should take into account expected changes (e.g. retirements) and make contingencies for the unexpected (e.g. resignations).

62. The organisational structure, roles and responsibilities should secure effective co-ordination and collaboration between all those involved, including contractors. Roles, responsibilities, accountabilities and performance standards for security at all levels should be clear and manage conflict with other business roles, responsibilities, accountabilities and objectives. All those with responsibilities for security should have authority and access to resources to discharge those responsibilities effectively. The organisation should ensure that proportionate governance and supervision of security at all levels is achieved. The design of jobs, processes and procedures should take account of those factors that affect reliable performance of the organisation.

63. Processes and systems should secure and assure maintenance of appropriate technical and behavioural competence of directors (both executive and non-executive), managers, leaders and all other staff and contractors with security roles and responsibilities.

64. Being a capable organisation requires the retention and use of knowledge so that security requirements are understood and risks are controlled throughout all activities, including those undertaken by contractors at all levels within the supply chain. An 'intelligent customer' capability should therefore be maintained to ensure that the use of contractors in any part of the organisation does not adversely affect its ability to manage security.

65. The organisation should sustain a design authority capability that includes suitable and sufficient experts with a detailed and up-to-date understanding of the security of the site, its facilities and their design, operation and security arrangements. Knowledge of the intended design performance of security equipment, processes and systems should be maintained to provide an adequate corporate memory and baseline for monitoring. This includes the need for an effective process to transfer and so retain knowledge from experienced staff leaving the organisation.

66. Knowledge should be captured and communicated within the organisation in a systematic, appropriate and reliable manner to all those who need to make security decisions. There should be provision for identifying, updating and preserving documents and records relevant to security. Such documents and records should be stored securely and should be retrievable and readable throughout their anticipated useful life (including statutory retention periods). Documents and records relevant to security should include those:

    (a) of value throughout the whole life of a facility;

    (b) that would assist during a security event;

(c) relevant to making future modifications; or,

(d) that could contribute to improvements in security.

3.1.3 SyDP 1.3 - Decision Making

FSyP 1 - Leadership and Management for Security	Decision making	SyDP 1.3
Decisions made at all levels in the organisation affecting security should be informed, rational, objective, transparent and prudent.		

67. Security should be given a high priority and this should be evident in all decision making processes. The processes should ensure that all relevant data and opinions are collected, recorded and considered, respecting and encouraging the contribution of those with divergent views. The processes should encompass means for setting security priorities to aid decision making at all levels. Security decisions should not be delayed unnecessarily (e.g. for commercial reasons) and personnel should be empowered to take timely decisions in the interests of security.

68. Decisions affecting security should consider the following factors (where relevant):

(a) the quality, accuracy and sufficiency of the information;

(b) the significance of uncertainties;

(c) the questioning of assumptions;

(d) exploration of all relevant scenarios that may threaten security;

(e) the range of options to appropriately manage risk in the short and long term;

(f) the criteria and standards that should be applied.

69. Decision making should be based on processes that ensure that conflicts between security and other business goals are recognised and appropriately resolved.

70. Decisions at all levels affecting security should also cater for the potential for error, uncertainty and the unexpected, and those taken in the face of uncertainty or the unexpected should be appropriately and demonstrably conservative.

71. Active challenge should be part of decision making throughout the organisation including at board and senior management levels. The organisation should encourage a questioning attitude from all staff and contractors. Though the form and function of the challenge will vary between different areas, designing-in appropriate active challenge mechanisms should be an inherent part of all decision making processes affecting security. Active challenge should:

(a) occur routinely as a result of a questioning attitude in the culture of staff and contractors;

(b) occur by design, and transparently, in all key decision making processes that may affect security;

(c) not originate solely from independent security assessment or peer review;

(d) assume that failure through inadequate design or implementation is possible, and be proactive in looking for ways that things could go wrong;

(e) be applied to technical/facility-based and management decisions; and

(f) be used in operational decision making in normal, threat and security event situations.

3.1.4 SyDP 1.4 - Organisational Learning

FSyP 1 - Leadership and Management for Security	Organisational Learning	SyDP 1.4
Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, security decision making and security performance.		

72. Organisations should have effective processes for seeking out, analysing and acting upon lessons from a wide range of sources. A learning organisation should challenge established understanding and practice by reflecting on experiences to identify and understand the reasons for differences between actual and intended outcomes. An absence of major security events does not necessarily indicate that risks are being adequately controlled and should not breed complacency. Near misses should be seen as opportunities to learn and a culture of open reporting should be fostered.

73. Learning should drive improvement throughout the organisation. Information should be collected from a range of sources inside the organisation, including from:

(a) workers (e.g. about strengths, weaknesses, deviations and errors, or concerns in relation to security procedures and processes);

(b) monitoring, review and audit of the implementation and effectiveness of governance, security strategies, policies, plans, goals, standards, processes and procedures;

(c) monitoring of security plant, systems and processes;

(d) testing, exercising and validation of security procedures under normal operational and threat conditions;

(e) inspections of sites, facilities, plant and equipment and other operational feedback systems;

(f) investigations of security events, specifically to ascertain immediate and underlying causes, including organisational, security management and cultural factors;

(g) self-assessments; and

(h) external assessments commissioned by the organisation.

74. Information should be sought actively and systematically from external sources, including from beyond the nuclear industry, to identify learning and improvement opportunities. Sources outside the organisation should include:

(a) reviews against international standards and practices;

(b) lessons from the investigation of events in other organisations from both within and outside the nuclear industry;

(c) benchmarking security performance, security management and learning methods and processes against those of other organisations from both within and outside the nuclear industry (e.g. CPNI, the National Cyber Security Centre and other UK government bodies and centres of excellence);

(d) security data, e.g. reliability data and general operating experience feedback; and

(e) feedback on security performance and issues from regulators.

75. Information from both internal and external sources should be analysed to identify trends and issues, e.g. Common Cause Failures (CCFs) or the influence of human or organisational factors, such as leadership and culture. The lessons learned should be embedded through a structured system for implementing corrective actions in a timely manner, which is rigorously applied and actively followed up to confirm completion. Effectiveness reviews should be undertaken to confirm that the changes have delivered the desired improvements. The learning processes and systems for implementation should themselves be subject to review and improvement.

76. The investigation of events, such as plant miss-alignment events, should include within their scope the potential for malicious activity to be the initiator. Trends should be reviewed alongside individual events to determine if deliberate actions are occurring on the site or facility. Suitable processes should be in place to ensure that the appropriate investigatory approach and techniques are applied where malicious activity is suspected.

3.1.5 SyDP 1.5 - Assurance Processes

FSyP 1 - Leadership and Management for Security	Assurance Processes	SyDP 1.5
There should be evidence-based assurance processes in place to inform strategy through the governance process, which welcomes challenge from across the organisation.		

77. The management system should ensure board-level assurance and oversight of the dutyholder's security performance, which should include compliance. A primary aim of assurance should be to provide ongoing confirmation that the security regime is delivering the required security outcome.

78. Governance and assurance cannot be effective unless the dutyholder is confident in their processes for performance assessment. This confidence can be secured through implementation of a suitable, evidence-based methodology, incorporating performance indicators, to support internal assessment of performance. In addition to monitoring performance, indicators should be used to correct adverse trends before security is impacted and to inform decision making. Dutyholders should therefore ensure that metrics and performance data are integrated with board-level processes to allow decision making at the right level in order to influence strategy and drive continuous improvement.

79. Analysis and interpretation of data are important in developing meaningful indicators. The set of indicators should draw from an appropriately wide and diverse range of sources, chosen so that the indicators provide meaningful information. Both leading and lagging indicators should be included and reliance solely on quantitative indicators should be avoided since the picture they create can be over-simplistic, therefore appropriate qualitative information should also be sought.

80. Metrics should be designed primarily to provide dutyholders with business information to inform strategy, rather than to assure regulators. In order to gain confidence in the efficacy of the metrics chosen, dutyholders should ensure that:

    (a) they are appropriate for the audience;

    (b) the rationale underpinning the metric is clear and understood;

    (c) they provide the board with information that they need to know;

    (d) there is clear cause and effect between the metric and the outcome/performance for which it is designed to provide information;

    (e) the dutyholder actually has the ability to impact on the variables being measured;

    (f) they are aligned with other relevant business metrics as appropriate;

    (g) there is broad coverage of functions and stakeholders (i.e. not simply covering similar aspects in different ways); and,

    (h) there is adequate focus on leading, not just lagging, indicators.

3.2 FSYP 2 - ORGANISATIONAL CULTURE

Fundamental Security Principle	Organisational Culture	FSyP 2
Dutyholders must encourage and embed an organisational culture that recognises and promotes the importance of security.		

81. Organisational culture encompasses the values and behaviours that contribute towards the social and psychological environment within a company. It represents the collective values, beliefs and principles of its employees and is influenced by factors such as history, industry, market, strategy and management style. Safety and security culture sit within and influence the wider organisational culture.

82. Security culture can be defined as 'The assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions which serves as a means to support and enhance nuclear security.'

83. While both nuclear safety and nuclear security consider the risk of inadvertent human error, nuclear security places additional emphasis on deliberate acts that are intended to cause harm. Because security deals with deliberate acts, security culture requires different attitudes and behaviour, such as confidentiality of information and efforts to deter malicious acts, as compared with safety culture. Accordingly, assurance of good safety and safety culture cannot be considered to provide assurance of good security and security culture, and vice versa.

84. An appropriate nuclear security culture aims to ensure that the implementation of nuclear security measures receives the attention warranted by their significance. Where it is embedded, nuclear security culture brings significant benefits to a nuclear security regime, providing greater assurance that the entire nuclear security system will accomplish its functions of deterring, detecting, delaying and responding to, theft, sabotage, unauthorised access, illegal transfer or other malicious acts involving radioactive material and the associated facilities and transport.

85. Safety and security cultures coexist and need to reinforce each other because they share the common objective of limiting risk, but there will be occasions where there are differences between safety and security requirements and these need to be carefully managed to ensure required outcomes are achieved. Therefore, successful organisational cultures foster an approach that integrates safety and security in a mutually supporting manner.

3.2.1 SyDP 2.1 - Maintenance of a Robust Security Culture

FSyP 2 - Organisational Culture	Maintenance of a Robust Security Culture	SyDP 2.1
Dutyholders should ensure that the board gives due priority to the development and maintenance of a security culture necessary to ensure the entire organisation recognises that a credible threat exists, nuclear security is important and the role of the individual in maintaining it is key.		

86. Dutyholders should commit to maintaining a strong security culture and communicating security expectations and standards to all staff and all parts of the

organisation and having the processes and arrangements in place to create and sustain this aspect of culture across the organisation and supply chain.

87. Dutyholders should also establish an appropriate, independent governance regime, led by the board to ensure that an adequate nuclear security culture is in place and it is maintained by the use of appropriate management systems/ structures. The methods and processes used for the maintenance of security culture should be subjected to internal assurance by security and operational staff that are Suitably Qualified and Experienced (SQEP). Furthermore, there should also be processes in place to review and test security culture across the organisation and its supply chain and mechanisms established that drive continuous improvement, tackle poor and inappropriate behaviour, enforce sanctions and encourage the sharing of relevant good practice.

88. A primary requirement should be setting out the security expectations and standards that need to be met, which should be communicated and understood by all staff. Therefore, roles, responsibilities and accountability for each level of the organisation responsible for security should be clearly defined and all staff should be accountable for compliance with all relevant aspects of the nuclear security regime.

89. The organisational culture should also support business and security priorities, be cognisant of HMG's priorities and be aligned to the organisation's own appreciation of risk. It is essential that any possible conflicts between the needs of safety and security are appropriately identified and addressed within the organisation's culture in a prompt manner.

90. Leaders can have a significant influence and therefore dutyholders should encourage leadership behaviour that supports and demonstrates a commitment to security culture. They should involve staff in decision making and ensure that sufficient resources are allocated to implement any assigned security responsibilities. The reporting of any event or matter that could affect nuclear security should also be encouraged.

3.3 FSYP 3 - MANAGEMENT OF HUMAN PERFORMANCE

Fundamental Security Principle	Management of Human Performance	FSyP 3
Dutyholders must implement and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately designed (to include tasks, competence staffing, workspace, equipment and administrative control), implemented and resourced.		

91. Human performance can be defined as a system that encompasses environmental, organisational and job factors and human and individual characteristics which influence behaviour at work in a way which can affect the ability to achieve the relevant security outcomes.

92. The human contribution to security can be positive or negative and may be made during design, construction, commissioning, operation, maintenance, modification or decommissioning. A systematic approach to understanding the role that humans play in delivering security and the factors that affect human performance is needed in order to minimise the potential for human error/violations/malicious acts to contribute to or escalate security events. This systematic approach to understanding the human contribution should be applied throughout the entire site/facility lifecycle.

93. It is essential that all personnel whose activities have the potential to impact on nuclear security are able to deliver their role reliably. Therefore robust arrangements for identifying reliance upon humans to deliver security and assuring that these actions are suitably supported is essential for an organisation to achieve secure operations.

94. Effective arrangements for the management of human performance typically include: identifying and analysing security tasks and roles, and then ensuring that these tasks are designed to match the information processing and physical capabilities of humans. This is achieved through ensuring:

- Adequate numbers of demonstrably competent staff are available and fit for duty;
- Staff operate in workspaces using equipment and interfaces designed to meet the demands of their tasks;
- Personnel are guided by well-designed administrative controls including normal and emergency security operating procedures.

95. The supporting delivery principles are relevant to both the enabling and operational fundamental principles and therefore should be considered as a whole and delivered via an integrated approach evidenced throughout the design, assessment and management of the security system.

3.3.1 SyDP 3.1 – Identification and Analysis of Security Tasks and Roles

FSyP 3 – Management of Human Performance	Identification and Analysis of Security Tasks and Roles	SyDP 3.1
A systematic approach to the identification and analysis of all tasks important to security should be undertaken, which demonstrates that tasks assigned to those with security roles are designed so that they can be effectively delivered.		

96. Dutyholders should systematically identify all tasks important to security and subject these to proportionate analysis to demonstrate that they are achievable taking into account likely operational conditions and requisite timescales where this is appropriate. This should apply to all personnel who deliver security functions, not only the security team.

97. The analysis should evaluate the demands these tasks place upon personnel in terms of perception, decision making and action. It should provide evidence to underpin the decision to allocate security functions to humans and should support the demonstration of a balanced design between human and engineered security measures avoiding an overreliance on the human to deliver security functions.

98. Task analysis should also demonstrate that tasks are designed taking account of human physical, physiological and psychological capabilities and limitations in order to achieve reliable and effective human performance.

99. The workload of personnel required to undertake tasks important to security should be analysed and demonstrated to be achievable. The ability of personnel to manage the workload required to maintain security during safety and security events should be demonstrated as part of security exercises and should be included in periodic security reviews.

3.3.2 SyDP 3.2 - Sufficency and Competence of Persons Delivering Security

FSyP 3 – Management of Human Performance	Sufficiency and Competence of Persons Delivering Security	SyDP 3.2
Dutyholders should demonstrate by analysis that they understand the numbers and competencies of personnel required to deliver all security functions, and that they have a systematic approach to identification of their training needs and competence management.		

100. Dutyholders should establish and maintain effective arrangements to ensure sufficient competent personnel are available at all times. Task analysis should be used where appropriate to define and justify the staffing design and staffing level (required number of competent personnel). This should include periods of normal operation, heightened threat levels and security event conditions. Once defined, staffing design and staffing levels should be demonstrated to be adequate via safety and security exercises and be subject to periodic review.

101. The security contingency plan should identify the number of security personnel and other site staff needed to address different types of security events, the skills they need and how deployment to and within the site or facility would be assessed and achieved in security event conditions. Deployment plans should cater for long-lasting

events, including those where there is severe local infrastructure disruption. On multi-facility sites the plans should describe how resources will be shared across the site.

102. A management process should be in place to ensure the fitness for duty of personnel to perform all security important tasks. This should address aspects such as fatigue arising from shift patterns and hours worked, and the effects of wider factors impacting fitness for duty, including occupational and other forms of stress, and drug and alcohol use.

103. The process for establishing training needs and competence management requirements for all those with security roles and responsibility for the delivery of security functions should be clearly defined. The process should include the phases of: job/task analysis; identification of competence requirements; training needs analysis; training programme design and implementation; formal assessment of competence; and training programme evaluation. The dutyholder should demonstrate they have a suitable training organisation to deliver competence management.

104. Dutyholders should demonstrate within their security plans that the competencies needed of each role and post-holder have been identified systematically. Security plans should also demonstrate how dutyholders assess and periodically re-assess the competence of workforce personnel who have security responsibilities. The frequency of reassessment should be determined by factors such as security significance, frequency of the task undertaken and operational experience.

105. Dutyholders should demonstrate that appropriate training records are maintained within a records management system that enables training to be planned, scheduled, delivered and monitored effectively, and SQEP status to be established when necessary.

106. The analysis of security roles and associated competencies may result in the identification and appointment of Duly Authorised Persons for Security Purposes (DAPSyPs) to control and supervise operations critical for security; and arrangements to ensure that only SQEP personnel perform any duties which may affect security.

3.3.3 SyDP 3.3 - Suitable and Sufficient Workspaces, Equipment and User Interfaces

FSyP 3 – Management of Human Performance	Suitable and Sufficient Workspaces, Equipment and User Interfaces	SyDP 3.3
Suitable analysis should be undertaken to demonstrate that workspaces, equipment and user interfaces are designed to match human capabilities, support reliable human performance and the delivery of security functions.		

107. The task environment in which personnel deliver security functions is comprised of a number of elements. This includes workspaces, such as security control centres, the physical environment and the equipment, tooling and Human Machine Interfaces (HMIs) used to monitor the security environment, determine security actions and carry them out. Good design is dependent on an integrated consideration of all elements of the task environment in order to promote situational awareness, vigilance and decision making.

108. Workspaces in which tasks important for security are completed should be designed taking into account the capabilities, characteristics and numbers of the intended users who will use the workspaces. In designing workspaces dutyholders should consider any requirements for the wearing and storage of protective clothing and use of tools and equipment.

109. Dutyholders should demonstrate that the physical arrangement of the workspaces (internal and external) have taken account of, and are compatible with, human perceptual and physical characteristics and limitations, as well as task demands, attributes and characteristics, and the need for communication and interaction between staff.

110. Environmental factors can increase both physical and mental stress, resulting in distortion or filtering of important sensory information, reduced vigilance and situational awareness, and increased human error potential and/or direct health and safety risks. Dutyholders therefore should demonstrate how environmental conditions in workspaces are controlled paying particular attention to the visual, thermal and auditory environment. Where environmental conditions cannot be controlled e.g. because security important tasks are completed outdoors, dutyholders should demonstrate how environmental impacts on human performance are minimised by the provision of suitable Personal Protective Equipment (e.g. inclement weather protection) or by staffing arrangements intended to maintain fitness for duty.

111. Where tasks important for security are performed using tooling and equipment or via human machine interfaces, dutyholders should demonstrate that these have been designed to ensure compatibility with the psychological and physical characteristics of the intended users and based on an understanding of the demands of the tasks they are used for.

112. Dutyholders should demonstrate that suitable and sufficient user interfaces including displays, alarms, communications equipment and controls have been provided to:

- Alert security personnel to the need take action in response to a security challenge;
- Allow personnel to understand the nature of the security challenge and determine an appropriate response;
- Execute appropriate actions in response to a security challenge including those needed to overcome failures of automated security systems or to reset a security system after its operation;
- Obtain feedback on actions taken and maintain situational awareness with respect to the impact of the security challenge on the security system; and
- Support communication between personnel located in the same or different operating locations, including locations external to the facility or site.

113. Dutyholders' security plans should demonstrate that where security functions are dependent on the human, the design of the task environment has minimised the likelihood of human error by accommodating the demands placed on personnel.

3.3.4 SyDP 3.4 – Suitable and Sufficient Procedures and Administrative Controls

FSyP 3 – Management of Human Performance	Suitable and Sufficient Procedures and Administrative Controls	SyDP 3.4
Dutyholders should demonstrate that sufficient procedures and administrative controls are provided, which are designed to minimise the likelihood of human error and support reliable delivery of security functions.		

114. All activities which may affect security should be carried out in accordance with written procedures which are in, or referenced within, the security plan.

115. Procedures to support security important tasks should be accurate and designed and presented in a format that is compatible with the needs of the intended user and suitable for the task that they are designed to support.

116. The dutyholder should demonstrate that it has a controlled process for the production, maintenance, review, amendment and version control of procedures. This should incorporate a process for validation and verification which includes end user involvement to confirm their technical accuracy and usability.

117. The dutyholder should demonstrate that it has a process of learning from experience to ensure procedures are appropriately revised based on use. It should also have mechanisms in place to ensure that procedure use and adherence is supported by the provision of good quality procedures and appropriate management oversight.

3.4 FSYP 4 - NUCLEAR SUPPLY CHAIN MANAGEMENT

Fundamental Security Principle	Nuclear Supply Chain Management	FSyP 4
Dutyholders must implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security.		

118. The Council of Supply Chain Management Professionals defines supply chain management as follows:

119. 'Supply Chain Management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies. Supply Chain Management (SCM) is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. It includes all of the logistics management activities noted above, as well as manufacturing operations, and it drives coordination of processes and activities with and across marketing, sales, product design, finance and information technology.'

120. SCM arrangements, which include control of procurement of items or services and contract management activities, are fundamental to ensure appropriate levels of control, oversight and assurance throughout all organisations within an organisation's supply chain. Effective SCM arrangements are designed to ensure that what is purchased complies with the purchaser's requirements (including contract specific requirements) and the technical specification which may be required for nuclear security related items or services. This is different to supply chain security, which seeks to ensure that aspects of confidentiality are maintained (See SyDPs 7.1-7.5).

3.4.1 SyDP 4.1 - Procurement and Intelligent Customer Capability

FSyP 4 - Nuclear Supply Chain Management	Procurement and Intelligent Customer Capability	SyDP 4.1
Dutyholders should maintain an 'intelligent customer' capability for all work carried out on their behalf by suppliers that may impact upon nuclear security.		

121. In addition to maintaining an 'intelligent customer' approach, dutyholders should retain overall responsibility for and oversight of, all work carried out on its behalf by contractors.

122. It is essential that dutyholders develop and maintain the capability to recognise work that may impact on nuclear security to ensure that it is subject to the appropriate procurement procedures underpinned by an effective commercial and/or supply chain strategy that is capable of delivering security plan requirements. The supply chain strategy, policy and arrangements should be appropriately resourced and subject to routine review to ensure that they remain effective and proportionate to the identified risks.

123. When procuring items or services that may impact on nuclear security, dutyholders should develop and issue specifications (for example the 'CPNI Guide to Producing Operational Requirements for Security Measures' (Reference 14)), that adequately describe the items or services, meet the security plan requirements and identify the required level of quality assurance.

3.4.2 SyDP 4.2 - Supplier Capability

FSyP 4 - Nuclear Supply Chain Management	Supplier Capability	SyDP 4.2
For work that may impact on nuclear security, dutyholders should evaluate and confirm that suppliers have the organisational and technical capability, capacity and culture to deliver items or services to the specification prior to placing any contract.		

124. Potential suppliers should be subject to a process designed to ensure that they have the capacity and security culture to deliver items or services to the specification prior to placing any contract for items or services that may impact on nuclear security.

125. Dutyholders' processes should also satisfy themselves that suppliers employ competent personnel, implement an appropriate quality management system and have adequate oversight of their own supply chain. Effective quality management systems ensure that items are fabricated, manufactured, installed, tested and inspected in a planned and controlled manner and that the required levels of performance are achieved.

3.4.3 SyDP 4.3 - Oversight of Suppliers of Items or Services that may Impact on Nuclear Security

FSyP 4 - Nuclear Supply Chain Management	Oversight of Suppliers of Items or Services that may Impact on Nuclear Security	SyDP 4.3
Dutyholders should conduct effective oversight and assurance of their supply chain.		

126. Dutyholders should establish arrangements for effective oversight and assurance of the supply chain, including the acceptance of items or services for work that may impact on nuclear security, supplied to or being undertaken on behalf of the dutyholder. Oversight should include measures to ensure contracts are reviewed, relationships are effectively managed and vendors are subject to thorough performance analysis.

127. There are parties who might wish to substitute counterfeit, fraudulent or suspect items for genuine items or services for commercial gain. Of equal (if not greater concern) is that parties may wish to incorporate a 'back door' to allow subsequent ease of access following installation. Such 'back doors' can create significant vulnerabilities. There is also the possibility that a party acting maliciously may wish to introduce a Trojan horse or other malicious code for subsequent exploitation of the system. Dutyholders and their supply chain should recognise these issues and have in place appropriate arrangements to mitigate them.

128. Dutyholders should also have arrangements in place to capture and act on operational experience feedback from its supply chain and supply chain management

activities, sharing learning as appropriate within the organisation, its supply chain and wider industry.

3.4.4 SyDP 4.4 - Commissioning

FSYP 4 - Nuclear Supply Chain Management	Commissioning	SyDP 4.4
Before bringing into operation or returning to service any facility, system or process that may affect security it should be subject to testing and a commissioning plan.		

129. A process for commissioning of security structures, systems and components should be identified in the security plan.

130. Dutyholders should ensure commissioning plans are produced that include a clear definition of roles and responsibilities, availability of resources and clearly defined milestones. Commissioning tests should:

    (a) demonstrate that, as built, the design intent claimed in the security plan (or operational requirement) has been achieved;

    (b) collect baseline data for equipment and systems for future reference;

    (c) validate those operating instructions etc. for which the commissioning tests provide representative activities and/or conditions; and

    (d) familiarise the operators with the operation of the facility or process.

131. The commissioning tests should be designed to identify any snags remaining following the design, manufacture, or construction/installation stages. However, the commissioning tests should not be used as the main means of identifying such errors.

132. Commissioning should be more than a demonstration that the plant will work. It should also include security tests as a key step in assuring security. The tests should be designed to demonstrate that the plant and associated security systems provide the intended degree of protection against threats, including human errors. Equipment designed to mitigate worst case Design Basis Threat (DBT) attacks should be tested as far as practicable during commissioning testing.

133. The security plan should be reviewed and updated in the light of the results of the commissioning tests and of any modifications made to the design or intended operating procedures that result.

THIS PAGE IS INTENTIONALLY BLANK

3.5 FSYP 5 - RELIABILITY, RESILIENCE AND SUSTAINABILITY

Fundamental Security Principle	Reliability, Resilience and Sustainability	FSyP 5
Dutyholders must design and support their nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle.		

134. Security structures, systems and components need to be designed to deliver their required security functions with appropriate reliability, according to the categorisation for theft and sabotage, and so provide confidence in the robustness of the overall design of the protective security system.

135. Designs that incorporate redundancy reduce the effects of random failure, and the incorporation of diversity and segregation reduces the effects of common cause failure. Examples of diversity include differing working principles, sizes of equipment, manufacturers, components, and types of equipment that use different physical methods. A design which adopts these principles will be tolerant of random failure occurring anywhere within the systems provided to deliver each security function.

136. The application of the principles in this section may vary according to the categorisation and classification of the security structure, system or component in question.

137. Sustainability is defined by the set of objectives and implementing actions incorporated into the nuclear security regime to support its continuing effectiveness. If the nuclear security regime is to remain effective, its constituent parts must be sustained and supported over time to ensure it continues to achieve the required outcomes.

3.5.1 SyDP 5.1 - Reliability and Resilience

FSYP 5 - Reliability, Resilience and Sustainability	Reliability and Resilience	SyDP 5.1
Security structures, systems and components should be appropriately qualified, with design incorporating reliability and resilience through ‘failsecure’, redundancy, diversity and segregation, supported by sufficient resources and contingency arrangements.		

138. Dutyholders should ensure availability of sufficient resources to maintain continuity of security. Continuity arrangements, aligned to appropriate standards should be developed in order to maintain nuclear security, thus building resilience to facilitate a rapid and effective security event response and recovery programme.

139. Due account should be taken of the need for security structures, systems and components to be designed to be inherently secure, or to fail in a secure manner where it does not impact on safety.

140. Potential failure modes should be identified and mitigated, using a formal analysis where appropriate. Consideration should be given to spurious operation, insecure failure modes and how modes of failure can be predicted or revealed and then repaired. Essential services critical to the correct functioning of the security system

should be considered to be part of the same and as such are required to display appropriate levels of reliability and resilience.

141. Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components and security plans should demonstrate that the required level of reliability for their intended security function has been achieved. For Security Class 1 systems, where required reliabilities cannot be achieved due to common cause failure considerations, the security outcome should be achieved taking account of the concepts of diversity and segregation by providing independent security measures.

142. Where effective and rapid security response is required, automatically initiated, engineered security measures should be provided where possible. For requirements that are less demanding, or on a longer timescale, administrative security measures (e.g. those involving operator actions based on procedures) may be appropriate.

143. The measures whereby the claimed reliability of security systems and components will be achieved in practice should be stated. Evidence should be provided to demonstrate the adequacy of these measures. This should include a reliability analysis of both random and systematic failures. Assumptions made in the course of the reliability analysis should be justified.

144. Where reliability data is insufficient to support a claim, appropriate measures should be taken to ensure that the onset of failures will be detected, and that the consequences of failure are minimised. Such measures may, for example, include planned replacement after a fixed lifetime, or be achieved through a programme of examination, maintenance, inspection and/or testing.

145. During expected site and facility operations, no unrevealed single random failure, occurring anywhere within the systems provided to perform a security function, should prevent the overall achievement of a security outcome. Any system that is the principal means of fulfilling a Category A security function should, other than in exceptional circumstances, always be designed to meet the single failure criterion. However, other systems which make a contribution to fulfilling the same security function, but are independent of the principal system, do not necessarily need to meet the single failure criterion.

146. Where appropriate (for example Security Class 1 systems) qualification procedures should be applied to confirm that structures, systems and components will perform their allocated security function(s) in all Normal, Heightened, Exceptional and security event conditions identified in the security plan and for the duration of their operational lives. The qualification procedures should:

    (a) provide a level of confidence commensurate with the security classification of the structure, system or component.

    (b) address all relevant operational, environmental, threat and security event conditions (including worst case DBT scenarios).

    (c) include a physical demonstration that individual items can perform their security function(s) (e.g. performance based testing of the civilian guard force or CNC) under the conditions, and within the time, substantiated in the facility's security plan.

    (d) Allow for qualification by an alternative appropriately validated and verified analysis where physical demonstration is not possible.

3.5.2 SyDP 5.2 - Examination, Inspection, Maintenance and Testing

FSYP 5 - Reliability, Resilience and Sustainability	Examination, Inspection, Maintenance and Testing	SyDP 5.2
Security structures, systems and components should receive regular and systematic Examination, Inspection, Maintenance and Testing (EIMT).		

147. A process for in-service testing, inspection and other maintenance procedures of security structures, systems and components should be identified in the security plan.

148. The EIMT should be commensurate with the reliability required of each item and carried out in a manner, governed by procedures, and applying codes and standards appropriate to the class of the security structure, system or component. Such inspection should be of sufficient extent and frequency to give adequate confidence that degradation will be detected before loss of the security function to ensure continuing quality and reliability. Accordingly, EIMT should prove the outcome of the complete system and the security function of each functional group.

149. Where test equipment, or other engineered means, is used for EIMT, the extent to which they reveal failures affecting security functions should be justified. The test equipment, or other engineered means, should itself be tested at intervals sufficient to uphold the reliability claims of the equipment under test.

150. EIMT is part of normal operation and it should be possible to carry out these tests without any loss of any security function. In other cases, the security plan should justify that there will be sufficient compensatory measures in place at all times to ensure any risk is adequately mitigated. Furthermore, the potential for EIMT to be exploited by an adversary should be analysed and the risks so arising mitigated.

151. Where complete functional testing is claimed not to be appropriate, an equivalent means of functional proving should be adopted. In circumstances where this cannot be done, either additional design measures should be incorporated to compensate for the deficiency, or it should be demonstrated that adequate long-term performance would be achieved without additional measures.

152. The continuing validity of equipment qualification of security structures, systems and components should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity. Furthermore, security structures, systems and components should be subject to extraordinary EIMT and/or re-validation after any event that might have challenged their reliability.

3.5.3 SyDP 5.3 - Sustainability

FSYP 5 - Reliability, Resilience and Sustainability	Sustainability	SyDP 5.3
Dutyholders should ensure that the constituent parts of its nuclear security regime are sustained and supported over time to ensure it continues to achieve the required outcomes.		

153. Senior managers within dutyholder organisations should set priorities and identify the long-term financial resources needed (e.g. for asset replacement) in addition to on-going operational expenditure related to issues such as training, configuration management, asset care and maintenance.

154. Dutyholders should ensure effective management and planning in order to sustain the nuclear security regime through reviewing resources allocated for effective design, operation and maintenance.

3.6 FSYP 6 - PHYSICAL PROTECTION SYSTEMS

Fundamental Security Principle	Physical Protection Systems	FSyP 6
Dutyholders must implement and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack.		

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

156. Accordingly, these SyDPs are ordered in such a way that starts with a process of target identification for theft and sabotage, followed by a graded model of system design incorporating a security outcome and posture for the system and an assessment of effectiveness through vulnerability analysis.

157. SyDPs 6.5 - 6.7 are concerned with aspects particular to adjacent facilities, nuclear construction activities and transportation of NM.

3.6.1 SyDP 6.1 - Categorisation for Theft

FSyP 6 - Physical Protection Systems	Categorisation for Theft	SyDP 6.1
Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorisation for theft.		

158. Dutyholders should categorise their site and facilities for theft according to the quantities and forms of all NM and ORM held or used (refer to the theft categorisation tables at Annex A). For NM, this includes a categorisation in relation to proliferation (Table 1 and 2 of Annex A) and a security group in relation to dispersal (Table 3 and 4 of Annex A). For ORM, only the security group in relation to dispersal is relevant. This is essential to determine the required outcome for the protective security system and allow the graded approach to be applied.

159. Inventories can change due to a variety of reasons and therefore dutyholders should have processes in place to identify and manage potential planned or unplanned changes to the categorisation to ensure the appropriate PPS outcome is always achieved (refer to the PPS Posture and Outcome tables at Annexes C and D).

3.6.2 SyDP 6.2 - Categorisation for Sabotage

FSyP 6 - Physical Protection Systems	Categorisation for Sabotage	SyDP 6.2
Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorisation for sabotage.		

160. Dutyholders should categorise their site and facilities for sabotage by undertaking a process of vital area identification (refer to the sabotage categorisation table at Annex B). This is essential to determine the required outcome for the protective security system and allow the graded approach to be applied. Vital areas may be identified where there is no NM/ORM present, for example on generating power stations where systems are essential to maintain control, containment or cooling.

161. Inventories and/or vulnerabilities can change due to a variety of reasons and therefore dutyholders should have processes in place to identify and manage potential planned or unplanned changes to operations to ensure the appropriate PPS outcome is always achieved (refer to the PPS Posture and Outcome tables at Annexes C and D).

3.6.3 SyDP 6.3 - Physical Protection System Design

FSyP 6 - Physical Protection Systems	Physical Protection System Design	SyDP 6.3
Dutyholders should design and implement a physical protection system that builds defence in depth and meets the required security outcome based on the categorisation for theft and sabotage.		

162. Dutyholders should design and implement a PPS (incorporating functions such as deterrence, delay, detection, response and insider threat mitigation) that achieves the relevant security outcome, which is graded according to the consequence for theft and sabotage. The tables at Annexes C and D to this document determine and describe the required security outcome that a dutyholder should seek to achieve within their security plan.

163. The tables at Annexes C and E refer to indicative security postures. These postures are intended to provide complimentary guidance by describing typical qualities and characterstics that a PPS capable of meeting the associated outcome may commonly comprise. However, flexibility is allowed for innovative, bespoke solutions to be adopted where dutyholders have demonstrated, with confidence, that the required security outcome is achieved.

164. Security plans demonstrate how the overall security outcome is achieved and are underpinned by secure operations at the facility-level. Therefore, dutyholders may also develop and implement appropriate facility-level, detailed security plans and procedures that support the overall PPS outcome.

3.6.4 SyDP 6.4 - Vulnerability Assessments

FSyP 6 - Physical Protection Systems	Vulnerability Assessments	SyDP 6.4
Dutyholders should satisfy themselves that their physical protection system achieves the required security outcome through undertaking vulnerability assessments.		

165. Dutyholders should validate the efficacy of their PPS through the conduct of structured and systematic vulnerability assessments, which may utilise one or more proven methodologies such as: paper-based adversary sequence modeling, force-on-force exercises; tabletops, wargaming, simulation or Subject Matter Expert (SME) analysis.

166. Dutyholders should also use vulnerability assessments to identify potential weaknesses and to seek improvements to their physical protection system.

3.6.5 SyDP 6.5 - Adjacent or Enclave Nuclear Premises

FSyP 6 - Physical Protection Systems	Adjacent or Enclave Nuclear Premises	SyDP 6.5
Dutyholders should give mutual consideration to the effects of adjacent or enclave nuclear premises on the maintenance of nuclear security.		

167. Many nuclear sites are adjacent to, or in the case of tenants, part of another nuclear premises. In these instances, dutyholders should give consideration to any shared services or shared contingency/emergency arrangements and to the impact that one may have, as an external hazard, on the other. This requires the establishment of arrangements to ensure the sharing of information to achieve relevant and mutual outcomes.

168. Furthermore, dutyholders should demonstrate that a coherent, coordinated approach is being maintained towards all aspects of security (and emergency response) that may be influenced by the adjacent or enclave nature of the sites.

3.6.6 SyDP 6.6 - Nuclear Construction Sites

FSyP 6 - Physical Protection Systems	Nuclear Construction Sites	SyDP 6.6
Dutyholders should ensure that they implement a physical protection system 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.		

169. Dutyholders should implement a PPS for a construction site that counters the threat posed by the site to an adjoining operating nuclear site. They should also identify and mitigate against the introduction of defects or vulnerabilities which could compromise the security or safety of the nuclear facility once it starts operating.

170. The graded approach is equally relevant for construction activities and therefore dutyholders should also have in place phased, incremental enhancements to the

PPS aligned with construction progress, as larger construction plant is introduced, more workers are present and the sensitivity of the work increases.

171. It is imperative that dutyholders achieve the appropriate security outcome (as defined in Annexes C and D) as the categorisation for theft and sabotage increases. In that regard, dutyholders should ensure that the security arrangements for each phase (or facility on an existing site) are implemented for a period which allows them to be fully embedded and functioning with high reliability prior to the associated increase in site sensitivity (e.g. holdings of SNI, nature of construction work being undertaken) or categorisation.

3.6.7 SyDP 6.7 - Protection of Nuclear Material During Offsite Transportation

FSyP 6 - Physical Protection Systems	Protection of Nuclear Material During Offsite Transportation	SyDP 6.7
Dutyholders should maintain arrangements to ensure the protection of Category I-III quantities of nuclear material against theft and sabotage whilst in transit.		

172. As a signatory to the CPPNM, the UK is obliged to ensure the protection of NM against theft and sabotage whilst in transit. Therefore, dutyholders should implement a PPS that achieves the outcome appropriate to the categorisation for theft and sabotage of the NM being transported (refer to the PPS security outcome and posture tables at Annexes C and D). In accordance with NISR 2003, these arrangements should be detailed in a TSS and qualified, where appropriate in a transport security plan.

173. Notwithstanding the above, dutyholders should also comply with UK and international regulations for the transportation of NM/ORM that does not fall under the schedule to NISR 2003.

174. Additional information on the interpretation of SyAPs for Class B carriers can be found in the ONR publication ‘Nuclear Transport Security Guidance for Class B Approved Carriers’ (Reference 18).

3.7 FSYP 7 - CYBER SECURITY AND INFORMATION ASSURANCE

Fundamental Security Principle	Cyber Security & Information Assurance	FSyP 7
Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.		

175. This fundamental security principle describes ONR's expectations of how organisations within the civil nuclear industry and third parties handling SNI and other assets will apply protective security to ensure the civil nuclear industry can function effectively, efficiently and securely.

176. The National Cyber Security Centre (NCSC) defines cyber security as 'The protection of devices, services and networks - and the information on them - from theft or damage.' The IAEA uses a different term, computer security, which it defines as 'A particular aspect of information security that is concerned with computer based systems, networks and digital systems.' For the purposes of this document, NCSC guidance and IAEA NSS series publications, the two terms can be considered to be synonymous.

177. Comprehensive CS&IA reflects the UK's widest national security objectives and ensures that the most sensitive assets are protected. Effective Cyber Protection Systems (CPS) are capable of deterring, detecting, defending/defeating disruptive challenges (such as cyber attacks), facilitating mitigation of and recovery from, any adverse effects. Done correctly, it enables continued operations as intended and delivers services efficiently.

178. Risk management driven from Board level is fundamental to effectiveness. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to information and infrastructure to an acceptable level. An effective process takes account of any relevant statutory obligations and protections (e.g. the Data Protection Act, Freedom of Information Act and the Official Secrets Act).

179. These SyDPs and the associated CPS security outcomes do not specify particular processes but describe what good cyber security will look like. Dutyholders may consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure (CPNI), NCSC, the relevant sponsoring government department and other sources of good practice to shape their business specific approaches.

3.7.1 SyDP 7.1 - Effective Cyber and Information Risk Management

FSyP 7 - Cyber Security and Information Assurance	Effective Cyber and Information Risk Management	SyDP 7.1
Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively.		

180. Dutyholders should ensure that they have a mature understanding of the cyber security and information risks throughout their organisation, and the lifecycle of their activities, informed by the National Technical Authority and current threat intelligence (provided by HMG and other sources). This provides the foundation for a clearly

communicated set of cyber security policies, standards, procedures and arrangements which are based on business objectives and proportionate risk management.

181. Dutyholders should also establish mechanisms with other industry and government stakeholders and utilise trained specialists to analyse cyber threats, vulnerabilities, and potential impacts which are associated with nuclear operations and related information. A fundamental aspect of this is categorisation of both SNI (including IT used to store, process or transmit); and technology (which includes equipment and software used in connection with activities involving NM/ORM). The tables at Annexes F and G provide further guidance on the categorisation of SNI and technology.

182. The categorisation informs the design and implementation of a CPS (incorporating functions such as Identify, Protect, Detect, Respond and Recover) that achieves the relevant cyber security outcomes, which are graded according to the consequence of compromise. The tables at Annexes H and I to this document determine and describe the required cyber security outcomes that a dutyholder should seek to achieve within their security plan.

183. The tables at Annexes H and J refer to indicative cyber security postures. These postures are intended to provide complimentary guidance by describing typical qualities and characterstics that a CPS capable of meeting the associated cyber security outcomes may commonly comprise. However, flexibility is allowed for innovative, bespoke solutions to be adopted where dutyholders have demonstrated, with confidence, that the required cyber security outcomes are achieved.

184. The CPS should also be supported by design validation processes to ensure that cyber mitigations are, and remain effective and achieve the required security outcome through the conduct of regular review including cyber risk and vulnerability assessments.

3.7.2 SyDP 7.2 - Information Security

FSyP 7 - Cyber Security and Information Assurance	Information Security	SyDP 7.2
Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.		

185. A key priority is the establishment of an overarching programme of information assurance driven by the board.

186. In order protect information and associated assets (including equipment, software and relevant data), dutyholders should ensure that staff are well-trained, exercise good judgement, take responsibility and are accountable for the information and associated assets they control, including all partner information. This includes the establishment of mechanisms and processes to ensure assets are properly classified in accordance with all relevant Classification Policy (e.g. the NISR Classification Policy) (Reference 15) and are appropriately protected.

187. Cyber security controls should be effective, resilient, and should enable nuclear operations. Dutyholders should ensure that information assets which are stored, processed or transmitted by digital systems are appropriately secured by a CPS that achieves the required outcome and posture (refer to Annexes F and H). This includes

risks posed by portable media devices, particularly those with wireless and internet capabilities, which should be identified and appropriately managed.

188. Dutyholders should implement security arrangements that ensure proliferation risks associated with uranium enrichment technologies and equipment are effectively managed.

189. Similarly, the supply chain also introduces risks and dutyholders should develop and maintain appropriate assurance measures to ensure that SNI and associated assets managed by contractors, as part of a classified contract, is appropriately protected wherever it is held.

3.7.3 SyDP 7.3 - Protection of Nuclear Technology and Operations

FSyP 7 - Cyber Security and Information Assurance	Protection of Nuclear Technology and Operations	SyDP 7.3
Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.		

190. The delivery of nuclear operations relies on functional, secure and resilient systems and technology that are able to protect against, detect, respond and recover from cyber threats.

191. It is essential that dutyholders fully characterise their technology (which includes equipment and software utilised on nuclear premises in connection with activities involving NM/ORM) and apply appropriate risk informed security controls. Technology utilised in nuclear operations includes the following categories:

(a) Computer Based Systems Important to Safety (CBSIS)

(b) Computer Based Security Systems (CBSy)

(c) Nuclear Material Accountancy and Control (NMAC) Systems

(d) Basic Process Control & Instrumentation Systems (BPC&I)

(e) Any other digital technology systems as appropriate

192. Following identification and characterisation, dutyholders should implement a risk-informed, current and actively-managed CPS that achieves the required outcome (refer to Annexes F, G and H).

3.7.4 SyDP 7.4 - Physical Protection of Information

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.		

193. Dutyholders should put processes and plans in place, including those developed from the early stages of design, to determine appropriate physical security requirements

through planning and risk assessment. This should inform the implementation of internal and external security controls in a layered fashion. These controls should deter, detect and/or prevent unauthorised access and protect information and associated assets against forcible or surreptitious attack. These controls should be integrated with the CPS to ensure it achieves the required outcome (refer to Annexes F, G and H).

194. Additionally, dutyholders should implement substantial controls for controlling access and proximity to high risk operational technology (which may have been identified as a vital area) and information assets.

3.7.5 SyDP 7.5 - Preparation for and Response to Cyber Security Incidents

FSyP 7 - Cyber Security and Information Assurance	Preparation for and Response to Cyber Security Incidents	SyDP 7.5
Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber attack), non-malicious leaks and other disruptive challenges.		

195. Dutyholders should develop and test business continuity, cyber event response, and disaster recovery arrangements aligned to relevant standards, to maintain nuclear safety and security, building resilience to facilitate a rapid and effective response to, and recovery from cyber security incidents that align with the response strategies and postures defined in Annexes G and H. This includes the development and testing of cyber contingency plans that set out procedures to be followed during a cyber security incident, which may also be part of a blended attack, including procedures to immediately adjust security requirements around the Government Response Level system.

196. Dutyholders should also put processes in place to regularly review resilience planning for critical assets, particularly those identified as being important to maintain nuclear security or safety, or holding SNI.

197. Effective management structures should be established that ensure shared communications between HR and security teams and provide policies and procedures for detecting, reporting, responding to and handling cyber security incidents, including disciplinary measures that are well communicated and understood by staff.

198. Dutyholders should also implement reporting mechanisms that ensure compliance with NISR. Dutyholders may align these with any reporting obligations to other relevant authorities (e.g. BEIS, ICO).

3.8 FSYP 8 - WORKFORCE TRUSTWORTHINESS

Fundamental Security Principle	Workforce Trustworthiness	FSyP 8
Dutyholders must implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.		

199. Workforce trustworthiness is reliant on effective personnel security policy and procedures. CPNI describes personnel and people security as comprising of an integrated set of policies, procedures, interventions and effects which seek to enhance an organisation or site's protective security by:

a) mitigating the risk of workers (insiders) exploiting their legitimate access to an organisation's assets for unauthorised purposes;

b) optimising the use of the workforce (and, where appriporate, the public) to be a force multiplier in helping to prevent, detect and deter security threats; and,

c) detecting, deterring and distrupting external hostile actors during the reconnaissance phase.

It is important to distinguish this from personal security, which seeks to reduce the risks to the safety or well-being of individual employees.

200. Workforce trustworthiness arrangements include a programme of pre-employment screening and national security vetting to ensure personnel hold a clearance or may be subject to supervision appropriate to their level of access to NM/ORM or SNI. Pre-employment screening and national security vetting is supplemented with on-going personnel security to reduce the risk of insider activity and provide management oversight of the continued suitability of personnel to hold their level of clearance.

201. Within the context of SyAPs, the term workforce includes direct employees and the supply chain, including any subcontracting parties.

3.8.1 SyDP 8.1 – Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security

FSyP 8 - Workforce Trustworthiness	Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security	SyDP 8.1
Dutyholders should ensure that human resources, occupational health and security departments cooperate to facilitate effective screening, vetting and ongoing personnel security arrangements for the workforce.		

202. Effective personnel security controls require close cooperation between multiple departments and line managers. Dutyholders should therefore ensure that their supply chain and own HR, occupational health and security department appropriately cooperate when dealing with matters of pre-employment screening, induction programmes, cessation of employment, national security vetting and ongoing personnel security. This is essential to ensure that any relevant information, which may be of security significance (e.g. medical conditions with the potential to cause a

loss of consciousness; the application and management of caveats), is communicated and managed effectively. In that regard, security, HR and occupational health departments are “relevant personnel” within NISR and have legal responsibility in their respective specialisms, to effectively communicate and address concerns that may pose a risk to nuclear security

3.8.2 SyDP 8.2 - Pre-employment Screening and National Security Vetting

FSyP 8 - Workforce Trustworthiness	Pre-employment Screening and National Security Vetting	SyDP 8.2
Dutyholders should deliver the appropriate combination of recruitment checks and vetting to satisfy themselves of the honesty and integrity of their potential workforce. .		

203. In order to determine the appropriate level of vetting an individual requires dutyholders should establish and maintain processes to evaluate areas and roles of particular insider risk (for example those with access to certain categories of NM, vital areas, classification of SNI, or those with assigned security responsibilities). Dutyholders should also establish robust arrangements that manage delivery of pre-employment screening and national security vetting sponsorship in compliance with extant Cabinet Office guidance and any additional ONR requirements. It is therefore important that only dutyholders’ duly authorised personnel are authorised to approve pre-employment check applications, (and even then only where applications fall within ONR signing authorities) and to sponsor applications for national security vetting.

204. Though short-term visitors to site are not necessarily personnel requiring screening or national security vetting, dutyholders should also undertake appropriate checks and report any relevant visits.

3.8.3 SyDP 8.3 - Ongoing Personnel Security

FSyP 8 – Workforce Trustworthiness	Ongoing Personnel Security	SyDP 8.3
Dutyholders should implement and maintain on-going personnel security management, arrangements and procedures to remain assured about their workforce and to mitigate the risks from insiders.		

205. Dutyholders should implement and maintain effective ongoing personnel security arrangements that include regular security appraisals, promote an organisational culture conscious of security priorities, and drive workforce and line management engagement. This includes seeking assurance as to the efficacy of ongoing personnel security arrangements provided for its supply-chain and any subcontracting parties.

206. As part of the above, procedures should be in place that ensure ONR are notified, appropriate to the level of clearance held, of any relevant factors such as positive drug and alcohol tests (including any attempt to falsify results), disciplinary action, illnesses causing question on a person’s suitability to hold a security clearance, adverse media reports, criminality or other behaviours of concern or inappropriate actions relating to those in the workforce.

3.9 FSYP 9 - POLICING AND GUARDING

Fundamental Security Principles	Policing and Guarding	FSyP 9
Dutyholders must demonstrate effective guarding and policing arrangements, integrating the operations of relevant police forces (e.g. CNC, BTP) and security guard services.		

207. The primary function of the CNC is to contribute to the security regime at those places to which it is deployed. It does this by providing an armed response, that in combination with other security measures, is capable of denying unauthorised access to NM and preventing both the theft of NM and an act of sabotage that could result in radiological consequences. It also has a role in intelligence gathering and dissemination and working with law enforcement partners.

208. The CNC derives its powers from TEA 2004 and has jurisdiction at designated nuclear sites, within 5km of those sites and wherever it needs to be to safeguard NM. The Civil Nuclear Police Authority (CNPA), a statutory authority accountable to the Secretary of State for Business, Energy and Industrial Strategy, is responsible for ensuring that the Constabulary fulfils its responsibilities in an efficient and effective manner.

209. During a security event, the security organisation may be supplemented by the local police force, which also has responsibility to respond to the sites in respect of non-terrorist related criminality and civil disorder. Other police forces (notably BTP) may also have a role in the protection of NM/ORM.

210. Security guard services are employed to undertake the general security duties as described in the security plan such as searching, access control, patrolling and either deliver or enable the immediate response to a potential security event.

3.9.1 SyDP 9.1 - CNC Response Force

FSyP 9 - Policing and Guarding	CNC Response Force	SyDP 9.1
Dutyholders should facilitate CNC deployment that is appropriate to achieve the required security outcome.		

211. Dutyholders should understand and acknowledge the statutory responsibilities of the CNC and liaise closely on tactical and operational policing matters with other dutyholders who have a call on the same complement of CNC.

212. It is important that dutyholders participate fully in a process to create and maintain integrated plans covering operational and tactical policing matters with other relevant stakeholders (e.g. CNC, relevant police forces and other dutyholders sharing the same CNC complement). These plans should clarify command and control arrangements during a security event and be based upon a shared understanding of risks and threats. Dutyholders should also participate fully in a process to create and maintain a Service Level Agreement (SLA), memorandum of understanding, or similar, covering commercial and contractual obligations between the dutyholder and the CNC which will inform performance management activity.

213. Dutyholders should facilitate and support CNC operational activity (including training and exercising) required to deliver their contribution to the relevant PPS outcome; and provide an appropriate level of support to the CNC and other police forces in the discharge of their duties under the Coordinated Policing Protocol.

3.9.2 SyDP 9.2 – Local Police Operations in Support of the Dutyholder

FSyP 9 - Policing and Guarding	Local Police Operations in Support of the Dutyholder	SyDP 9.2
Dutyholders should facilitate local police forces' provision of support by way of assistance to the CNC or delivering a response to the site in respect of terrorist, criminal or protest activity.		

214. Dutyholders should understand and acknowledge the statutory responsibilities of relevant local police force(s).

215. It is important that dutyholders participate fully in a process to create and maintain integrated plans covering tactical and operational policing matters with local police forces. The plans should clarify command and control arrangements during a security event and be based upon a shared understanding of risks and threats and capability of the relevant police force to respond to such. Dutyholders should also facilitate and support the local police operational activity (including training and exercising) required to deliver their contribution to the relevant PPS outcome.

3.9.3 SyDP 9.3 – Security Guard Services

FSyP 9 - Policing and Guarding	Security Guard Services	SyDP 9.3
Dutyholders should employ civilian security guards to provide the unarmed guarding that conducts nuclear security operations as described in the site security plan such as patrolling, access control and searching; and, who deliver or enable the immediate response to a security event.		

216. Dutyholders should establish arrangements such that security guard services are appropriately resourced, fully integrated with the wider security, safety and event response (including clarity over command and control arrangements) and are driven by a shared understanding of threat and vulnerability assessments.

217. The operations of security guard services should be underpinned by a Service Level Agreement (SLA), contract of employment or similar, covering commercial and contractual obligations to maintain service delivery at all Government Response Levels, shift resilience, and define metrics which will inform performance management activity.

218. Dutyholders should also facilitate and support security guard service operational activity (including training and exercising) required to deliver their contribution to the relevant PPS outcome.

3.10 FSYP 10 - EMERGENCY PREPAREDNESS AND RESPONSE

Fundamental Security Principles	Emergency preparedness and response	FSyP 10
Dutyholders must implement and maintain effective security emergency preparedness and response arrangements which are integrated with the wider safety arrangements.		

219. The objective of Emergency Preparedness and Response (EP&R) planning is to take all reasonably practicable measures to prepare for possible security events at nuclear facilities, and to mitigate their consequences should they occur. Proper application of emergency preparedness and response arrangements should ensure, with high confidence, that radiological consequences arising from a nuclear security event are minimised. The emergency preparedness and response arrangements should also be designed to consider severe nuclear security events beyond the design basis threat and ensure that the consequences of these will be mitigated to the extent that is within the dutyholders' control.

220. FSyP 10 states that dutyholders must maintain integrated security and safety EP&R arrangements. A key principle of this integration is considering nuclear events to be cause agnostic until the initiator is confirmed.

3.10.1 SyDP 10.1 – Counter Terrorism Measures, Emergency Preparedness and Response Planning

FSyP 10 - Emergency Preparedness and Response	Counter Terrorism Measures, Emergency Preparedness and Response Planning	SyDP 10.1
Dutyholders should have in place incremental counter terrorism measures that can be implemented in response to changes in threat; and, EP&R arrangements to deal with any nuclear security event arising and the potential effects.		

221. Counter terrorism measures and EP&R planning arrangements for nuclear security events should be driven by threat assessments, the DBT and incorporate a range of functions including: security contingency planning, immediate response, event and consequence management, maintaining situational awareness, effective command, control and communications. Dutyholders should also establish measures to deliver an appropriate, incremental response to changes in the government response level system.

222. The dutyholder's arrangements should be set out primarily in a nuclear security contingency plan (or similar), which forms part of the security plan, but is integrated with other site emergency plans in order to deliver a coherent, timely and effective response to a range of events. Security EP&R planning arrangements should be driven by the legal requirement, threat assessments, the DBT and the assets to be protected from theft and sabotage.

223. Plans should consider the following arrangements: anticipation of resource requirements, assessment of threats, immediate response to a nuclear security event, command, control and communication procedures, integrated event and consequence management and alignment with other plans.

224. Nuclear security event management strategies should be developed to manage escalation and to restore control. The dutyholder's security contingency plans should be used to form a suitable basis for developing these strategies with the ultimate aim of returning the facility and/or site to a stable, safe and secure state.

225. The strategies and plans should identify all the procedural support requirements that will be needed during a nuclear security event. The procedures should define all the roles and responsibilities needed for an effective nuclear security event response. The plans and procedures should be fully integrated, with supporting agencies participating in the design and subsequent acceptance of the procedures and specified tasks. Effective storage arrangements should be in place to ensure the timely availability of these plans and procedures in nuclear security event conditions.

226. The infrastructure, systems and equipment identified for the delivery of emergency arrangements and nuclear security event management should be of appropriate robustness, suitably maintained and tested, and readily available at all times. However, the emergency operating procedures should be written recognising the potential practical difficulties (e.g. adversary action, radiation levels, poor lighting, access issues and communication system failures) that could reasonably be encountered in security event conditions.

227. The EP&R arrangements should also be designed to consider severe security events beyond the design basis threat and ensure that the deployment of supporting agencies are understood and can be supported. Additionally, plans should cater for long-lasting nuclear security events, including those where there is severe local infrastructure disruption. On multi-facility sites the plans should describe how resources will be shared across the site.

3.10.2 SyDP 10.2 - Testing and Exercising the Security Response

FSyP 10 - Emergency Preparedness and Response	Testing and Exercising the Security Response	SyDP 10.2
Dutyholders should implement a regime of exercising to train personnel and test the efficacy of the nuclear security contingency plans.		

228. Security emergency arrangements should be appropriately trained, practised, exercised and tested by dutyholders in order that all personnel with roles and responsibilities are capable of delivering the appropriate response in a timely, cohesive and effective manner. Additionally, supporting agencies should, where possible, be included in training and exercising in order that a more effective and timely response in operationally challenging environments is delivered.

229. Security emergency arrangements should be exercised and tested regularly. The exercises should be chosen so that in total they test the full scope of the site's arrangements and activities within the plans.

230. Dutyholders should implement procedures to ensure that operational learning is identified, captured and arrangements amended accordingly in a timely manner.

3.10.3 SyDP 10.3 - Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event

FSyP 10 - Emergency Preparedness and Response	Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event	SyDP 10.3
Dutyholders should implement structures and processes to ensure effective command, control and communications arrangements during and post nuclear security events.		

231. Dutyholders should establish a robust and resilient command, control and communications capability, integrated with all relevant stakeholders. This capability should include, for example: a central alarm station, emergency control room, main control room and security force control centre, as appropriate. The on-site emergency control room should be provided from which an emergency response can be suitably and safely directed. This should be located such that the likelihood of its non-availability due to the nuclear security event is minimised. However, when movement of emergency response personnel is limited due to the nature of the nuclear security event, dutyholders should be capable of delivering emergency management from any location.

232. In the plan of multi-facility sites, where one or more such centres may be provided, appropriate command, control and communication arrangements should be put in pla e to ensure a co-ordinated response.

233. Dutyholders should also plan to facilitate and support an integrated multi-agency post-event recovery, including the management of post-event crime scenes in support of the CNC, local police and other deployed agencies and responders.

234. Where strategic centres are provided (on or off site), the security plan should recognise the need for coordinated interactions to support responding agencies during nuclear security events, to receive information and briefings, and to support the response with government.

THIS PAGE IS INTENTIONALLY BLANK

4 KEY SECURITY PLAN PRINCIPLES

235. This section contains principles that should be applied across the breadth of the FSyPs and SyDPs. Collectively, it brings together a range of topics that should be considered when assessing the security plan for a facility and/or site.

236. The principles apply across a wide range of facilities of differing type and categorisation for theft and sabotage. Applying these principles therefore requires judgement and proportionality in deciding which principles are relevant to the situation being assessed and then whether enough has been done in relation to each applicable principle.

4.1 KSYPP 1 - SECURE BY DESIGN

Key Security Plan Principles	Secure by Design	KSyPP 1
The underpinning aim should be an inherently secure design, consistent with operational purposes.		

237. ‘Secure by Design’ is an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. It mitigates specific threats by using an approach, design or arrangement tailored to address malicious acts. For example the threat of a vehicle borne improvised explosive device can be designed out by making the building impervious to such an attack or through installing hostile vehicle mitigation measures that prevent any vehicular access within a requisite standoff distance. Inherent security is not the same as ‘passive security’.

238. Inherent security can be improved by:

(a) reducing the inventory of NM/ORM or SNI to the minimum necessary to achieve the required function of the facility and removing NM/ORM or SNI no longer required;

(b) controlling the physical state of NM/ORM or SNI (for example by vitrification of high active wastes or encryption of stored data) to remove or minimise their potential effects if compromised; and

(c) application of engineering, administrative or technical security measures.

Such measures can be articulated within a hierarchy of controls thus:

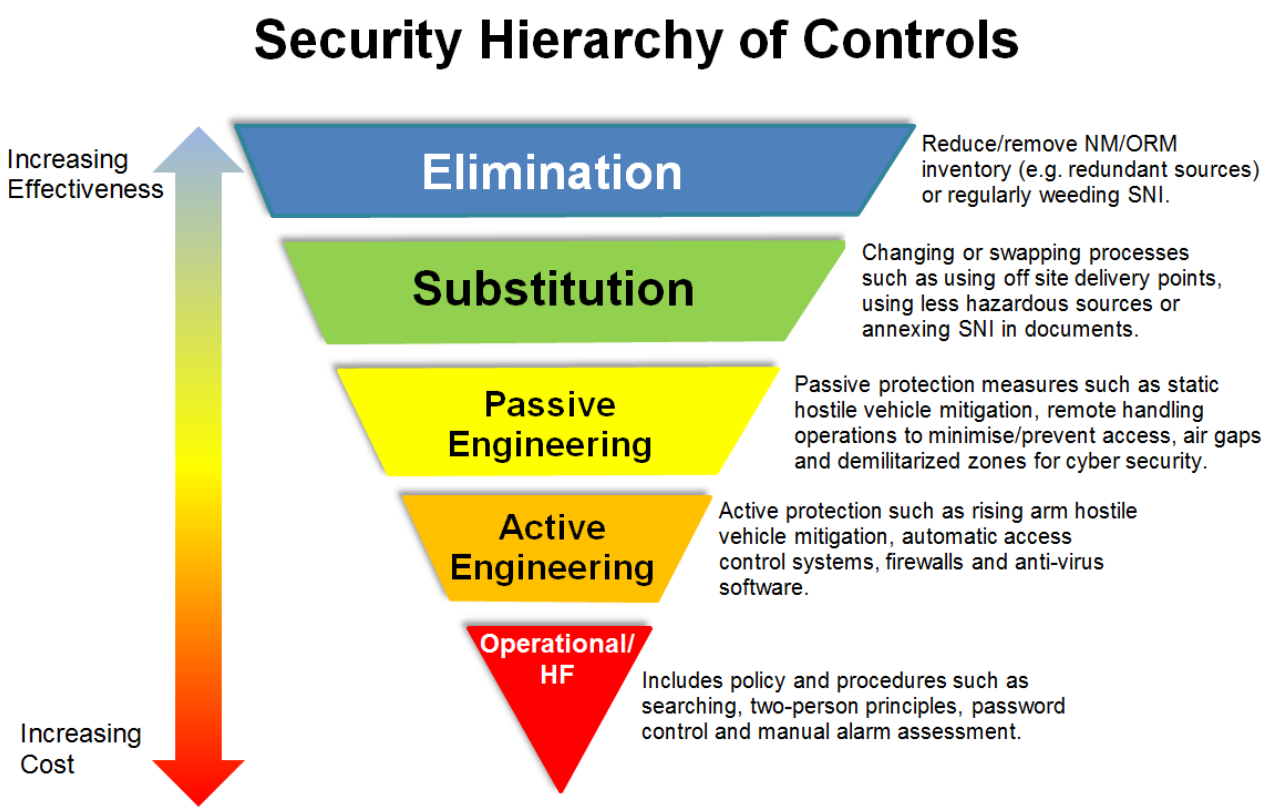

Figure 4 – The Secure by Design Hierarchy of Controls

239. Application of this hierarchy should reduce the need for, and reliance on, protective security systems and the challenges placed on them. In addition to this hierarchy, security by design for cyber can be further enhanced by the following underpinning principles:

- **Principle 1: Focus on what's critical.** Designs should include only those system functions that are essential to operations.
- **Principle 2: Move key assets out-of-band.** Designs should ensure that systems differentiate between user and attacker access for any given function and build in adequate separation (logical, physical or both).
- **Principle 3: Detect, react, adapt.** Designs should employ dynamic sensing and response technologies.

4.2 KSYPP 2 - THE THREAT

Key Security Plan Principles	The Threat	KSyPP 2
Protection systems should be designed, evaluated and tested using the state's Design Basis Threat, which is supported by threat intelligence that provides situational awareness in order to facilitate dynamic response to new and emerging threats and inform security strategy.		

Design Basis Threat

240. It is essential that a DBT is used as the basis for the design, evaluation and testing of protection systems to seek assurance that it will meet a defined security outcome.

Within the UK, the DBT malicious capabilities assessed as confronting the civil nuclear industry and assumptions about the composition and capabilities of malicious actors posing a threat are described in detail in the current DBT document, issued by BEIS. The DBT, which incorporates assessment provided by the relevant government authorities (e.g. The Joint Terrorism Analysis Centre (JTAC)), is updated and amended in line with IAEA recommendations. It should be used in conjunction with the assessment principles within this document to ensure that protection systems are designed to provide an appropriate level of defence in line with the graded approach against attempts to:

(a) steal NM or ORM in use, storage or transit in order to construct;

i. an Improvised Nuclear Device (IND). The possibility exists that the theft, including repeated theft of small quantities of plutonium, high enriched uranium or uranium-233, could lead to the construction of an IND by a technically competent, well-resourced terrorist group. INDs incorporate nuclear materials designed to result in the formation of a nuclear-yield reaction; or

ii. a radiation exposure device, which incorporates radioactive and/or NM and is designed to intentionally expose members of the public to radiation; or

iii. a radiological dispersal device, which is designed to spread radioactive and/or NM using conventional explosives or other means; or

(b) carry out an act of sabotage against a site holding NM or ORM, or against a transportation of NM or ORM, in such a manner as to create a radiological consequence.

(c) Compromise SNI and/or technology (including equipment and software utilised on nuclear premises in connection with activities involving NM/ORM) in order to facilitate or commit acts of theft or sabotage.

241. When considering the DBT, dutyholders must give due attention to one of the most serious threats facing the civil nuclear industry, which is ‘insiders’. The IAEA define the term ‘insider’ as ‘one or more individuals with authorised access to nuclear facilities or NM in transport who could attempt unauthorised removal or sabotage, or who could aid an external adversary to do so’. The threat from an insider poses a unique problem due to the advantages they have over an adversary that does not have authorised access.

Threat Intelligence

242. The DBT for the civil nuclear industry is reviewed annually and revised every three years. The IAEA recognises that new or emerging threats may additionally require immediate consideration and actions. Therefore, to work in conjunction with the competent authority, dutyholders should develop, manage and maintain a proportionate threat intelligence (TI) capability in order to meet the challenges of a changing physical and cyber threat landscape and generate an appropriate intelligence-led response. This is important to both fields as threats are often inherently linked, and dutyholders should use physical and cyber threat reporting on an on-going basis, within a demonstrable framework that supports an on-going security program.

243. It is incumbent on dutyholders to fulfil this role by drawing information and intelligence from a wide range of internal and external sources through the coordination of a systematic collection effort to support prioritised business intelligence requirements to provide situational understanding to generate risk based responses. This is achieved through the application of an iterative process that converts raw data and information into intelligence through a structured series of actions. The aim is to supplement the DBT through the timely conveyance of predictive and actionable TI that can be used to facilitate specific outcomes focused on the delivery of effective security strategy and secure operations that support maintenance of the overall the nuclear security regime.

232. In order to ensure that TI processes are effective and consistent, they should be:

- Governed by a documented planning and review cycle which is proactively developed by dutyholders to service their specific business requirements.
- Supported by identification of dutyholders' key assets, vulnerabilities and on-going assessment and monitoring of adversary intent and capability towards the organisation.
- Informed by intelligence collection from a range of internal and external sources, with assessments authored by analytical teams with a multi-disciplinary skillset.
- Actionable, timely and designed to service the requirements of different audiences from board to engineer to back office employee.

244. Dutyholders should make themselves aware of the threats facing them and implement a threat reporting strategy to deliver threat assessments to protect them. The use of TI is a dynamic on-going process that needs to be effectively designed and managed and dutyholders must weigh the relative importance of TI requirements in light of their current priorities, capabilities, budget and security plans.

245. Planning, generating, consuming, analysing, disseminating, and responding to TI reporting can be expensive. Dutyholders of different sizes, budgets and staffing levels will have varying capabilities to undertake TI. As with other regulatory expectations, inspectors should ensure that they are mindful of proportionality through the graded approach when assessing the adequacy of a dutyholder's TI processes (i.e. effort and expenditure on TI should be representative of the threats faced by the organisation and the potential impacts of any incident).

Integrating Threat Reporting

246. The principles and structures involved in TI processes are equally applicable to the personnel, physical and cyber security arenas and should not be addressed in stovepipes. Whilst expertise in these areas is likely to be distinct, convergence in these functions and fusion of threat reporting around them is vital to foster a holistic threat picture to complement the DBT and is integral to a coherent security risk management program. It should inform situational understanding of the threat environment and ensure key management comprehend the overlap between associated threat vectors and the ways in which these can manifest in blended attacks (e.g. insider activity, close access operations). This will enable continuous improvement based on the emerging threat landscape to inform the dutyholder risk-based decision making process to support security operations and defence in depth planning.

4.3 KSYPP 3 - THE GRADED APPROACH

Key Security Plan Principles	The Graded Approach	KSyPP 3
Protection systems should be based on a graded approach, taking into account the categorisation for theft or sabotage of NM/ORM, and consequence of compromise of any SNI.		

247. There are a wide range of hazards associated with different facilities and activities on nuclear premises so the depth and rigour of the analysis required will vary considerably. This is consistent with ONR's Enforcement Policy Statement (Reference 16) in that the requirements of security should be applied in a manner that is commensurate with the risk. Therefore, the extent and detail of assessments undertaken by dutyholders as part of a security plan or other security submission, including their independent assessment and verification, need to be commensurate with the categorisation for theft and sabotage or holdings of SNI. Similarly, subject to other legal duties or public policy requirements, ONR regulatory attention should likewise be commensurate with the categorisation for theft and sabotage or holdings of SNI, although aspects including novelty, uncertainty and dutyholders' compliance history will also be factors.

248. Security plans, and the analysis and assessments contained within them, must be suitable and sufficient for the purpose of identifying all relevant threats, vulnerabilities, any associated consequences and measures to manage and mitigate the risk.

249. Dutyholders are responsible for undertaking a target identification of their facilities in order to determine the categorisation for theft and sabotage and any holdings of SNI. The higher the categorisation, the more rigorous and comprehensive the analysis should be, leading to greater defence in depth of protection. In contrast, a low category facility may require a more limited analysis and be provided with fewer or less extensive security provisions.

250. The SyAPs assist inspectors in judging whether, in their opinion, the dutyholder's security plan has satisfactorily demonstrated that the requirements of relevant legislation can be, or have been, met. The guidance associated with each principle gives further interpretation on their application and more detailed information is available in technical assessment guides also published by ONR.

251. The fundamental expectation for security plans is that they should demonstrate that risks are proportionately managed, security is adequate and the normal requirements of good practice in security design, security operations and security management are met. They should also set out how risk assessments have been used to identify any weaknesses in the proposed security arrangements' design and operation and detail any corrective action within a security improvement schedule, or identify where improvements were considered but discarded. They should also show that security is not unduly reliant on a disproportionately small set of specific security features and where appropriate is supported by the safety case

252. In light of the above, protection systems should be designed using a graded approach, taking into account the DBT, vulnerabilities, the relative attractiveness, nature and categorisation of any NM/ORM or the consequences of compromise of any SNI. A graded approach should be used to provide higher levels of protection against security events that could result in higher consequences.

253. The application of the graded approach should be carried out comprehensively and consider all applicable principles, with all relevant risks considered as a combined set. Therefore, priority should be given to achieving an overall balance of security rather than satisfying each principle, or making a risk management judgement against each principle. When judging whether the graded approach has been applied appropriately, it may be necessary to take account of safety risks in addition to nuclear security risks and justify that an appropriate balance has been achieved. Inspectors will be proportionate in what they require from designers and dutyholders.

4.4 KSYPP 4 - DEFENCE IN DEPTH

Key Security Plan Principles	Defence in Depth	KSyPP 4
Protection systems should reflect a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary and ensure appropriate mitigation of security events should prevention fail.		

254. International consensus is that the appropriate strategy for achieving an overall security outcome is through the application of the concept of defence in depth. Protective systems reflect this concept by incorporating a series of independent layers and methods (for example structural, other technical, personnel and organisational) of protection that have to be overcome or circumvented by an adversary in order to achieve their objectives.

255. An important aspect of the implementation of defence in depth is the provision of multiple, and where appropriate, independent, barriers across a range of protection functions such as deterrence, detection, delay, assessment, response, access control and insider threat measures, to protect NM/ORM and nuclear facilities against acts of theft or sabotage, or compromise of SNI. This is the barrier model of defence in depth, as shown in the diagram below.

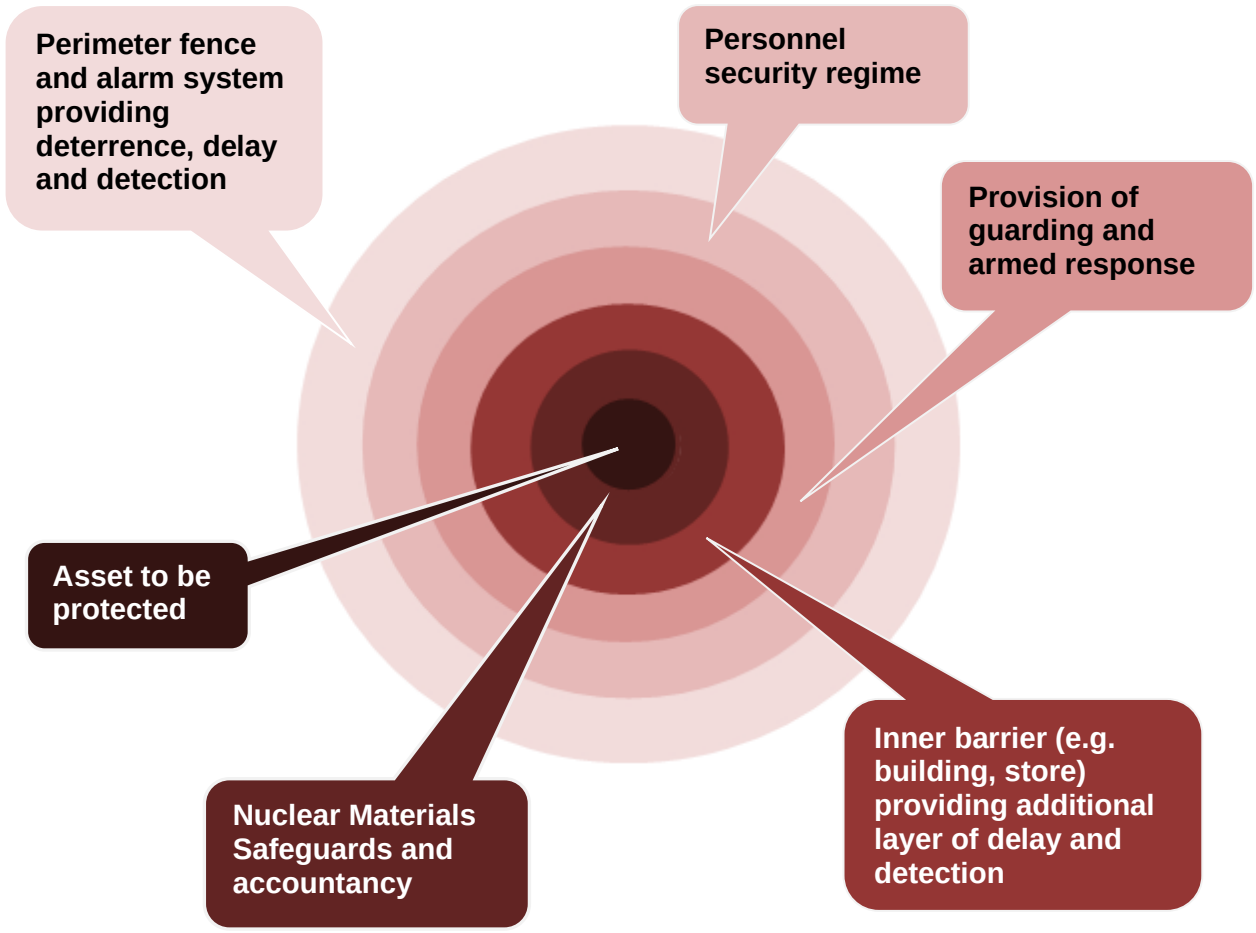

Figure 5 – Layered Model of Security Defence in Depth

256. Whilst defence in depth incorporating multiple barriers should be designed to prevent an adversary being successful, the application of defence in depth levels also underpins nuclear security, particularly mitigation of security events should prevention fail. The five levels of defence in depth are described below:

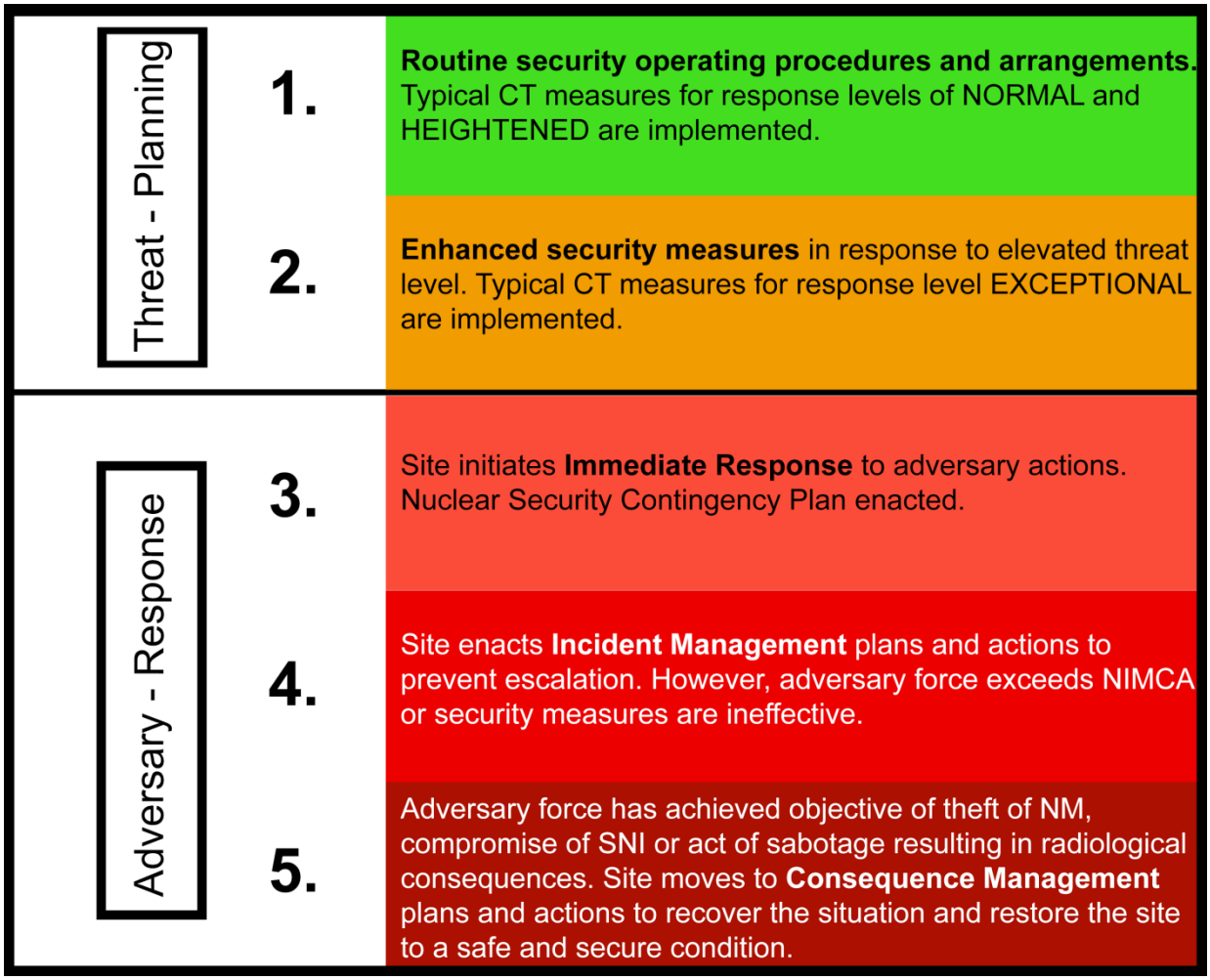

Figure 6 – The Five Levels of Security Defence in Depth

4.5 KSYPP 5 - SECURITY FUNCTIONAL CATEGORISATION AND CLASSIFICATION

257. Effective implementation of the security aspects sought by SyAPs relies upon a number of general principles and related measures aimed at ensuring the reliability and capability of a site's and/or facility's security measures. For instance, it is important that structures, systems and components, including software for instrumentation and control, are classified on the basis of their security significance. For designs under development, the security classification may be an iterative process, with preliminary assignments of the security class of structures, systems and components needing to be finalised using vulnerability analysis. It is important that all structures, systems and components are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.

4.5.1 KSyPP 5.1 - Security Categorisation

Key Security Plan Principles	Security categorisation	KSyPP 5.1
The security functions to be delivered at a dutyholder's site and facilities, in all modes of operation, should be identified and then categorised based on their significance with regard to security.		

258. The identification of security functions should follow a systematic approach and be based on the security plan, target analysis and adversary paths arising from a DBT attack, including those posed by insiders. This should result in a list of security functions (e.g. deterrence, detection, delay and response) derived appropriate to counter the threat. The security functions identified should be sufficiently detailed to support subsequent security classification activities and to facilitate a clear demonstration in the security plan of their effective delivery.

259. The security functional categorisation scheme employed should be linked explicitly with the security outcome that a site or facility is expected to achieve (refer to the tables in Annexes C and D). These principles suggest dutyholders should consider implementing a categorisation scheme on the following basis:

(a) Category A (SyC A) – any nuclear security function that needs to achieve Fortified posture for Outcome 1 or 2.

(b) Category B (SyC B) – any nuclear security function that needs to achieve Robust posture for Outcome 2 or 3.

(c) Category C (SyC C) – any nuclear security function that needs to achieve Routine posture for Outcome 3 or 4.

260. The method for categorising security functions should take into account:

(a) the consequence of failing to deliver the security function;

(b) the extent to which the security function is needed, either directly or indirectly, to prevent, protect against or mitigate the consequences of a security event;

(c) the potential for a functional failure to realise a serious vulnerability or exacerbate the consequences of an existing security event; and

(d) the likelihood that the function will be called upon.

261. The categorisation of security functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components that deliver the security functions.

262. Where the security functions might be affected by safety considerations, the design process should seek to treat security and safety in a complementary manner. The process should aim to ensure that the measures designed for one will also serve the interests of the other. In particular, safety and security measures should be designed and implemented in such a manner that they do not compromise one another.

263. The categorisation assigned to each security function should be used to classify the structures, systems and components that deliver the function.

4.5.2 KSyPP 5.2 - Security Classification

Key Security Plan Principles	Security Classification	KSyPP 5.2
Structures, systems and components that have to deliver security functions should be identified and classified on the basis of those functions and their significance to security.		

264. Where security functions are delivered or supported by human action, these human actions should be identified and classified on the basis of those functions and their significance to security. The methods used for determining the classification should be analogous to those used for classifying structures, systems and components outlined in the following paragraphs.

265. Methods for classifying the security significance of structures, systems or components should be based primarily on the vulnerability assessment and adversary action sequence analysis, taking due consideration of any deterministic and probabilistic methods that underpin a concept of operations, final denial positions or final points of detection. The method can be complemented, where appropriate by SME judgement and opinion, with account taken of factors such as:

    (a) the category of security function(s) to be performed by the item;

    (b) the likelihood that the item will be called upon to perform a security function;

    (c) the potential for a failure to encourage a malicious act, induce a vulnerability or exacerbate the consequences of an existing security event, including situations where the failure affects the performance of another system, structure or component; and,

    (d) the time following any initiating threat at which, or the period throughout which, it will be called upon to operate in order to bring the facility to a stable, secure and safe state.

266. A number of different security classification schemes are in use in the UK. The following scheme, linked to the categorisation scheme above, is recommended in these principles:

    (a) Class 1 (SyC 1) – any structure, system or component that forms a principal means of fulfilling a Category A security function.

    (b) Class 2 (SyC 2) – any structure, system or component that makes a significant contribution to fulfilling a Category A security function, or forms a principal means of ensuring a Category B security function.

    (c) Class 3 (SyC 3) – any other structure, system or component contributing to a categorised security function.

267. The availability and reliability of the security measures should be commensurate with the categorisation for theft and sabotage and their security functions within the defence in depth hierarchy. In particular, mitigating security measures should not be regarded as a substitute for security by design or protection barriers, but as further defence in depth.

268. Appropriately designed interfaces should be provided between (or within) structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to mitigate the propagation of compromise should be assigned to the higher class.

269. Auxiliary services (including essential services) that support components of a system important to security should be considered part of that system and should be

classified accordingly unless failure does not prejudice successful delivery of its security functions.

4.6 KSYPP 6 – MANAGING CHANGES TO SECURITY STANDARDS, PROCEDURES AND ARRANGEMENTS

Key Security Plan Principles	Managing Changes to Security Standards, Procedures and Arrangements	KSyPP 6
The dutyholder should have a robust process for managing changes to security standards, procedures and arrangements that includes assessing the impact of any proposed change if inadequately conceived or executed, identifying associated risks and implementing suitable control measures.		

270. To demonstrate adequate control of changes to the security Standards, Procedures and Arrangements (SPAs) described in the security plan and to achieve compliance with NISR 2003 Regulation 6 and 7, dutyholders should develop proportionate change management processes. These should be based on a sound understanding of the security significance of the impact on security if the change is inadequately conceived or executed, (this may be informed by a categorisation and classification process as per KSyPP 5 or similar). This is important in ensuring that there is adequate scrutiny and challenge in developing any proposed change to extant SPA; security risk is effectively managed through the provision of appropriate security mitigation throughout the change lifecycle from design to operations; and, SPA will continue to deliver security outcomes described in the approved SP.

271. Change can be temporary or permanent and result from factors including site operations, movement or change in inventory, changes/updates to the Nuclear Baseline etc. Regardless of what prompts any change to SPA, a dutyholder's processes for managing should:

- be consistent, robust, incorporated into the management system and applied to all activities that have the potential to impact nuclear security if inadequately conceived or executed;
- require staff involved in all aspects of managing change to be competent for their role;
- be owned and embedded throughout the organisation, up to and including the board/executive team or equivalent senior managent;
- reference the Nuclear Baseline (or equivalent) as a starting point to assess the potential impact and include a process for updating it on a regular basis;
- include an initial screening assessment (determined by a reasonably conservative understanding of the impact on security and consequences) which identifies the potential security significance of a proposed change, if inadequately conceived or executed, thus helping to categorise it and establish appropriate internal justification and challenge levels;
- identify suitable compensatory measures to ensure nuclear security is not adversely affected throughout the lifecycle of the change;

- take into account the interdependencies and aggregate effect of multiple changes; and,
- include robust governance and assurance processes;
- be subject to periodic review on the effectiveness of the overall arrangements and the changes that have been implemented.

4.7 KSYPP 7 - CODES AND STANDARDS

Key Security Plan Principles	Codes and standards	KSyPP 7
Structures, systems and components that are important to security should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate codes and standards.		

272. Appropriate national or international codes and standards (e.g. BSI, ISO, MFES) should be adopted for security structures, systems or components. The codes and standards applied should reflect the functional reliability requirements of the structures, systems and components and be commensurate with their security classification.

273. Codes and standards should underpin design commensurate with the importance of the security function(s) being delivered. Each code or standard adopted should be evaluated to determine its applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the relevant security function(s).

274. The combining of different codes and standards for a single aspect of a security structure, system or component should be avoided. Where this cannot be avoided, the combining of the codes and standards should be justified and their mutual compatibility demonstrated.

275. Where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar security significance, should be adopted. Alternatively, the results of operational experience, tests, analysis, the judgement of SMEs or a combination thereof, should be applied to demonstrate that the structure, system or component will perform its security function(s) to a level commensurate with its classification.

276. Certain security functions are delivered by systems that are not amenable to analysis and codification (e.g. guard response, searching). In these instances, it is possible to achieve the required levels of quality assurance by performance testing, provided the sample is large enough, is representative of the range of operating conditions and periodically reassessed.

THIS PAGE IS INTENTIONALLY BLANK

5 THE REGULATORY ASSESSMENT OF SECURITY PLANS

5.1 OVERVIEW OF ASSESSMENT

277. These principles set the foundation for effective security plans. If the principles are adopted by dutyholders, it will help them achieve 'right first time security plans' which will facilitate ONR assessment, thereby reducing regulatory impact. During assessment, inspectors should use the principles proportionately, and make judgements commensurate with the categorisation for theft and sabotage and the holdings of SNI. There are eight interrelated security plan principles that address:

(a) the production process;

(b) outputs;

(c) lifecycle aspects;

(d) characteristics;

(e) optimism, uncertainty and conservatism;

(f) content and implementation;

(g) maintenance; and,

(h) ownership.

278. ONR's assessment process consists of examining security submissions to enable a judgement to be made that security risks to an existing or proposed facility are controlled according to a graded approach, through implementation of an appropriate security posture and demonstration that the required security outcome has been achieved. ONR's assessment covers an examination of the claims, arguments and evidence. A submission may relate to a plant modification to part of a facility or to equipment within a facility as part of a temporary security plan.

279. A diagram showing the relationship between Claims, Arguments, Evidence and SyAPs is provided below.

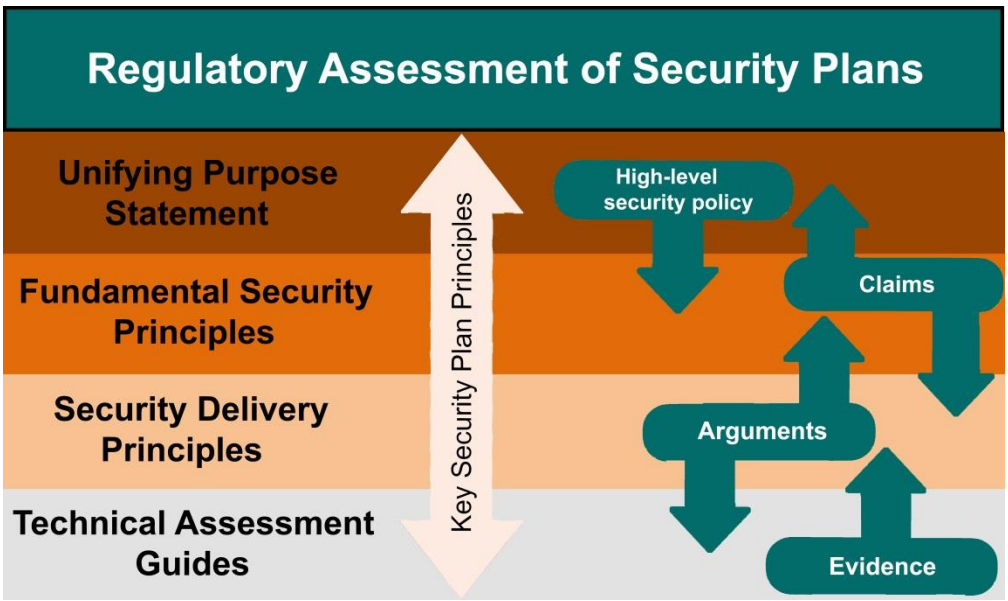

Figure 7 – Diagram Showing the Relationship of Security Assessment Principles with Claims, Arguments and Evidence in Security Plans

280. ONR's assessment involves the examination of documentation and arrangements which demonstrate the security of a facility and its processes, operations and organisation. In addition, it can also involve inspection of the facility to verify the accuracy of the security plan as a description of the facility, its assumptions, security provisions and requirements. ONR also undertakes compliance inspections to determine whether the arrangements needed to implement these provisions and requirements have been implemented appropriately. These examinations and inspections are important in establishing confidence in the reliability of the information and conclusions presented in the security plan along with its currency and efficacy.

281. ONR uses a sampling approach in deploying its resources and not every security plan is assessed fully in every respect. The extent of the sample and any subsequent approval decision taken in light of the security plan will take into account:

    (a) the level of confidence ONR has in the dutyholder's process for producing security plans;

    (b) the level of confidence ONR has in the dutyholder's approach to leadership and management for security;

    (c) the risks and vulnerabilities associated with the activities covered by the security plan; and

    (d) recent events or operating experience at the facility, or similar facilities.

282. Other important factors in ONR's approval decisions include:

    (a) the extent to which the dutyholder has taken all appropriate measures to remove or minimise inventories of NM/ORM or SNI; or minimise any sabotage vulnerabilities it has identified;

    (b) the extent to which the dutyholder has demonstrated that the security outcomes, posture and regulatory requirements have been met, including the application of relevant good practice in security design, operation and management;

    (c) the acceptability of the depth, completeness, accuracy and detail of the dutyholder's security plan, in relation to the nature of the facility and the categorisation for theft and sabotage and holdings of SNI;

    (d) the dutyholder's level of knowledge concerning processes (e.g. transportation and outages) and their effects on security;

    (e) the confidence ONR has in the conclusions reached by the dutyholder as influenced by the effectiveness and maturity of the dutyholder's governance and assurance processes; and.

    (f) the extent to which the dutyholder has demonstrated compliance in relation to pre-employment screening and national security vetting arrangements with HMG guidance, as supplemented by other ONR requirements, in its role as a Vetting Authority.

283. ONR will use the findings from its assessment of the security plan to inform its inspection and approval priorities and enforcement activities.

284. The principles in this section cover how security plans should be produced and managed, what they need to do and what they should contain. This section also expands on ONR's philosophy of security plans and explains what to look for in terms of good points and pitfalls if they are inappropriately applied, or their limitations misunderstood.

285. A security plan is a logical and hierarchical set of documents that describes risk in terms of the categorisation for theft and sabotage of the facility or site and the modes of operation, potential vulnerabilities, and those security measures that need to be implemented to prevent or mitigate them. It should demonstrate that the physical protection system achieves the required security outcome and can be operated and maintained in a secure manner. It takes account of experience from the past, and sets expectations and guidance for the processes that should operate in the future if security is to be delivered successfully. The security plan clearly articulates the linkage from security claims through arguments to evidence.

286. The documented security plan becomes the basis for security arrangements, informing the activities and behaviours of the people who interact with the facility. In this context there are two key user groups of the security plan. Firstly, there are those who interact directly with the facility. These include the security staff and operators who deliver security at the site or facility, as well as those who maintain any security function. The second set is the company directors (and senior managers) who are accountable for the security of their site and who rely on the security plan for accurate and objective information on control measures to make informed business decisions. Therefore, the security plan and the identification of risk management options should be recognised as essential elements of the dutyholder's business processes. The security plan should not be used to retrospectively justify an argument for design decisions or business decisions that have already been made.

287. The production of a security plan does not in itself ensure the security of a site or facility. Instead, starting with a proper understanding of the security plan, the technical and procedural requirements deriving from it must be properly implemented so that the facility can be operated and maintained in a secure manner.

5.2 SECURITY PLAN PRODUCTION

288. The process of analysing security requires SME insight, where people can envisage the variety of routes by which vulnerabilities can be exploited (e.g. adversary sequence modeling) once targets have been identified. A range of security measures or controls can then be identified, from which the most appropriate can be selected and implemented. Security analysis requires an extensive understanding of the facility and its safety case, both in the present and foreseeable future, its profile in a variety of conditions (e.g. during movements of NM/ORM, outages and shutdown) and experience of security events (including at other facilities) together with the measures adopted to prevent their recurrence.

289. It also requires an understanding of how people and organisations may affect security. Structured and systematic assessment is required to identify potential failure modes arising in protective security systems and opportunities for control and, if necessary, mitigation. Since all of this knowledge is unlikely to be found in a single individual, a structured and collective approach is required to enable the aggregation of the necessary expertise, both in developing the security plan and implementing its requirements. The inspector should look for evidence of all these attributes.

290. Security depends on a variety of attributes and control measures working together reliably to mitigate the security risks at a site or facility. Therefore, the organisational

systems (e.g. interactions between people) are just as important as the technical security systems, particularly bearing in mind that protective security systems and organisations can have more failure modes than technical physical security equipment. This starts with the system (process) for producing security plans, which needs to be reliable and robust.

5.2.1 RASyP 1 - Security Plan Production - Process

The Regulatory Assessment of Security Plans	Security plan production process	RASyP 1
The process for producing security plans should be designed and operated commensurate with the categorisation for theft or sabotage of NM/ORM and consequence of compromise of any SNI.		

291. Application of this principle should result in:

(a) a clear specification for the purpose, standards and expectations of each element of the process;

(b) defences or barriers being designed to mitigate against failure of the process;

(c) monitoring and testing of the production process to ensure each element is functioning to the expected quality;

(d) responsive feedback mechanisms to ensure that significant issues over the quality of individual security plans are reviewed to check for underlying or systemic defects or weaknesses in the process; and

(e) definition of the training and qualifications needed for the formal roles within the process (to ensure that those who undertake the roles are suitably qualified and experienced).

292. The process used to produce security plans needs to deliver consistently good quality plans. In this context, ‘to produce’ encompasses all elements of the process including initial optioneering, writing the plan, and any means of verification or review. For a security plan to claim that the facility under consideration is secure or highly unlikely to be compromised, the process used to derive such claims needs to have commensurate reliability.

293. The different elements of the security plan process should be defined clearly, including their purpose and key features, and their potential weaknesses or failure modes. The defences or barriers in response to the identified potential failures or weaknesses should be determined. To achieve the necessary high reliability in the process, consideration should be given to some form of diversity in the elements and their defences, not just redundancy. This should include security plan review by people who are independent of those involved in its production. The independent review function (among others) should seek to identify defects in the security plan process, not just address issues relating to the content of the security plan itself.

294. The design of the security plan production process and the means of monitoring and testing the adequacy of its defences or barriers to failure should utilise lessons from major failures and successes of security management systems or security plan processes, including those from outside the nuclear industry. In particular, specific

measures should be in place to guard against known ‘common cause failures’ of the process (e.g. resource constraints, programme pressures, commercial drivers and incentive schemes) that can result in poor quality or incomplete security plans and inadequate identification or management of the risks. Adopting a quality plan approach will help to reduce such issues.

295. During times of high stress (e.g. tight deadlines, intense commercial or operational pressure), additional measures should be considered to protect the quality of the security plan. The regular monitoring and testing of the security plan process should provide for such periods of increased stress and not just be restricted to normal situations.

5.2.2 RASyP 2 - Security Plan Production - Outputs

The Regulatory Assessment of Security Plans	Security plan process outputs	RASyP 2
The security plan process should produce security plans that facilitate secure operations that are aligned with business processes.		

296. The process for producing security plans should take into account the needs of those who will use the security plan to ensure disciplined, secure operations. It is essential that the security plan documentation is clear and logically structured so that the information is easily accessible to those who need to use it. This includes designers, security delivery and maintenance staff, technical personnel and managers who are accountable for security.

297. The security plan process should also take into account how the different levels and types of documentation fit together to cover the full scope and content of the security plan. The needs of users should be addressed by ensuring that all descriptions and terms are easy to understand by the prime audience, all arguments are cogent and coherently developed, all references are easily accessible, and that all conclusions are fully supported, and follow logically from the arguments. The trail from claims through argument to evidence should be clear.

5.3 RASYP 3 - SECURITY PLAN LIFECYCLE ASPECTS

The Regulatory Assessment of Security Plans	Lifecycle aspects	RASyP 3
For each lifecycle stage, the security of NM/ORM, nuclear facilities and SNI should be demonstrated by a valid security plan that takes into account the operational experience from previous stages and for future stages.		

298. Security of NM/ORM, nuclear facilities and SNI should be demonstrated in a security plan before any associated risks materially exist. The security plan for each stage should take account of future lifecycle stages, i.e. it should build on the security plan for previous stages and show that the security intent for subsequent stages will be achieved. Any constraints that apply in all subsequent stages should be detailed in the security plan in which they are identified. The security plan for decommissioning should have been considered in all previous lifecycle stages. In the event of early, unplanned permanent shutdown of a facility, the security plan should be revised to

address any security implications arising from the early shutdown and to identify any changes to the strategy and timescales for decommissioning.

299. The specific content and depth of information in a security plan will vary from stage to stage, and should be commensurate with the nature of the particular stage and inter-relationships with other stages. For example, in the early stages (e.g. design concept), the security plan will be more a statement of future intent, claims and principles, whereas a security plan for an operational stage would be expected to contain far more detail, evidence and analysis.

5.4 RASYP 4 - SECURITY PLAN CHARACTERISTICS

The Regulatory Assessment of Security Plans	Security plan characteristics	RASyP 4
A security plan should be accurate, objective and demonstrably complete for its intended purpose.		

300. A security plan should:

(a) Set out a dutyholder's commitment to meet their legal obligations under NISR;

(b) include the dutyholder's organisational structure and ownership;

(c) explicitly set out the argument for why security risks are controlled according to the graded approach;

(d) link the information necessary to show that security risks are controlled according to the graded approach, and what will be needed to ensure that this can be maintained over the period for which the security plan is valid;

(e) support claims and arguments with appropriate evidence, and with experiment and/or analysis that validates performance assumptions, which may include SME opinion;

(f) refer to any major ongoing or planned security enhancements;

(g) describe the risk management strategy (covering physical, personnel and CS&IA);

(h) accurately and realistically reflect the proposed activity, facility and its structures, systems and components;

(i) detail the security personnel assets and procedures, including issues relating to primacy and responsibility;

(j) identify any limits and conditions necessary in the interests of security; and,

(k) identify any other requirements necessary to meet or maintain the security plan such as surveillance, maintenance and inspection.

301. To achieve these, a security plan should:

(a) identify the site and facility's categorisation for theft and sabotage by a thorough and systematic process;

(b) identify any vulnerabilities through a thorough and systematic threat and threat sequence identification process (e.g. adversary sequence modeling);

(c) articulate claims, arguments and evidence that the facility conforms to relevant good security practice and sound security principles. For example, security at a nuclear facility should be designed cognisant of the DBT, using the concept of 'defence in depth' by adopting the security posture identified within the physical protection system principles. Instances where good practice has not been met should be identified and justification provided why alternative approaches are adequate or suitable;

(d) provide sufficient information to demonstrate that security has been applied in an appropriate manner. For example, it should be clearly demonstrated that all security structures, systems and components have been designed, constructed, commissioned, operated and maintained in such a way as to enable them to fulfil their security functions for their projected lifetimes;

(e) demonstrate that the required security outcome has been achieved; and,

(f) provide the basis for the secure management of people, plant and processes. For example, the security plan should address management and staffing levels, training requirements, maintenance requirements, operating and maintenance instructions, and contingency and emergency instructions.

302. The essence of these aspects may be distilled within a 'security case' or similar, for further expansion and justification by claims, arguments and evidence. Further guidance on these topics is set out in the relevant section(s) of these principles.

303. To demonstrate that vulnerabilities are being managed appropriately and arrangements implemented according to the graded approach, the security plan should:

(a) provide evidence justifying the criteria used in decision making or option selection;

(b) justify the options chosen in terms of meeting relevant good practice, together with any discarded options.

5.5 RASYP 5 - SECURITY PLAN OPTIMISM, UNCERTAINTY AND CONSERVATISM

The Regulatory Assessment of Security Plans	Optimism, uncertainty and conservatism	RASyP 5
Security plans should identify areas of optimism and uncertainty, together with their significance, in addition to strengths and any claimed conservatism.		

304. The security plan should present a balanced view of the level of knowledge and understanding, and of the resultant risks. It should provide a proportionate justification that includes appropriate conservatism but without undue pessimism. Otherwise, it can mislead those who need to use the security plan to take decisions on risks and on managing security. An unbalanced plan will also fail to identify areas where more work might be needed, either to support the current conclusions or to provide a valid basis for any subsequent work if the security plan needs to be revised

(e.g. due to a modification or a change that affects the security operating regime or procedures). This principle encompasses optimism and uncertainties in the design of a security system and in the basis of the security plan (e.g. analytical methods and codes, underlying assumptions, adversary sequence modeling and time delay margins). Areas of uncertainty should be offset by appropriate levels of conservatism.

305. To ensure that risks are understood and can be managed appropriately, potential vulnerabilities in the design of the security plan should be identified clearly (e.g. in the summary or main conclusions of the security plan). Mitigating measures that have been or can be applied to address the weaknesses should also be identified. It should also be made clear within a security improvement schedule, how any outstanding security significant issues are being, or will be, addressed.

5.6 RASYP 6 - SECURITY PLAN CONTENT AND IMPLEMENTATION

The Regulatory Assessment of Security Plans	Security plan content and implementation	RASyP 6
The security plan should identify all aspects of operation and management required for achieving and maintaining security and how these will be implemented.		

306. Aspects of operation and management likely to be important for achieving and maintaining security are highlighted in individual sections of these principles. These have not been written to be exhaustive.

307. The security plan should justify how the security arrangements identified within it will be implemented effectively. The means of implementation considered should include:

(a) any limits and conditions required to ensure that the facility is operated securely at all times;

(b) identification and allocation of the resources required to deliver the security plan;

(c) the security procedures and instructions that need to be followed;

(d) the required examination, inspection, maintenance and testing regimes justified in or assumed by the security plan;

(e) control, supervision, qualification and training and other security management requirements;

(f) operational changes needed to respond to varying threat levels; and

(g) inputs to the nuclear security contingency plan and integration with the wider site emergency planning arrangements.

5.7 RASYP 7 - SECURITY PLAN MAINTENANCE

The Regulatory Assessment of Security Plans	Security plan maintenance	RASyP 7
A security plan should be actively maintained throughout each of the lifecycle stages, and reviewed regularly.		

308. An effective security plan should be:

(a) recorded in a dynamic suite of documents, easily accessible and understandable by those who need to use them;

(b) managed through formal processes; and

(c) reviewed periodically on a defined basis.

309. The security plan needs to be kept up to date to meet the needs of all its users. In particular, the knowledge used at the time of writing the security plan needs to be supplemented by subsequent monitoring of site and facility e.g. from commissioning, operation, periodic inspection and testing, research or experience from other facilities. The security plan may need periodic update and renewal as the DBT evolves. The security plan will also need to be updated to take account of changes at the facility, the site and its surroundings, for example:

(a) changes arising from modifications or revised operating methods or processes;

(b) changes to facility risks (e.g. resulting from changes to type and form of NM inventory)

(c) changes arising from security events, operating experience, examination or testing results,

(d) changes from updated design or analysis methods, research findings or other new information arising from external sources, particularly government sources;

(e) the outcome from periodic and interim security reviews;

(f) changes due to plant or facility ageing; and,

(g) changes in the immediate vicinity of the facility (e.g. from external factors such as adjacent construction activity).

310. Annual reviews of security ensure that the cumulative impact of modifications and changes have been considered so that the security plan remains valid and up to date. Annual reviews should be supplemented with a deeper and more searching review which includes comparison with current modern standards. These reviews should be comprehensive and carried out on a longer timescale as specified in dutyholder arrangements. They should identify any appropriate security improvements and timescales for implementing them.

311. Reviews of security events, operating experience and other sources of information should not be restricted to the facility or site in question. They should include similar

sites, facilities or security equipment and also a wider range of nuclear and industrial experience, both nationally and internationally where available.

5.8 RASYP 8 - SECURITY PLAN OWNERSHIP

The Regulatory Assessment of Security Plans	Security plan ownership	RASyP 8
Ownership of the security plan should reside within the dutyholder's organisation with those who have direct responsibility for security and where possible based at the location holding the risk.		

312. The primary purpose of a security plan is to provide the dutyholder with the standards, procedures and arrangements required to enable secure management and operation of the site, facility or activity (such as transportation of NM) in question, and therefore it should be understandable, useable and clearly owned by those with direct responsibility for security.

313. Ownership and responsibility require:

(a) an understanding of the security plan, the standards applied in it, its assumptions and the limits and conditions derived from it (i.e. intelligent customer capability);

(b) the technical capability to understand and act upon the security plan work produced by others;

(c) the ability to use the security plan to manage security and ensure that the risks from activities are mitigated according to the graded approach;

(d) that users of security plans be involved in their preparation to ensure that they reflect operational needs;

(e) processes in place to ensure that amendments to security plans are made in accordance with NISR 2003; and,

(f) that the plan is fully implemented at the facility and that those involved in its implementation can challenge elements of the plan to confirm its effectiveness in achieving the desired outcomes.

6 GLOSSARY

TERM	DEFINITION
adversary action sequence	A required/ordered series of acts performed by an adversary to achieve their objectives
access control	Means to ensure that access to assets is authorised and restricted based on business and security requirements
access delay	The element of a physical protection system designed to increase adversary penetration time for entry into and/or exit from the nuclear facility or transport.
adversary	Any individual performing or attempting to perform a malicious act. The term threat is used to refer to a postulated adversary against which security measures are designed, wheras an adversary is active and requires an immediate response.
adversary path	An ordered collection of actions against a target that, if completed, results in successful theft or sabotage
adversary sequence modeling	Using an analytical model to estimate the probability of success of an adversary taking a specific path or set of paths.
attack	An attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
authentication	The provision of assurance that a claimed characteristic of an entity is correct.
authorisation	The granting by a competent authority of written permission for operation of an associated facility or for carrying out an associated activity, or a document granting such permission.
authorised person	A natural or legal person that has been granted an authorisation. An authorised person is often referred to as a "licensee" or "operator".
carrier	Any person, organization or government undertaking the carriage of nuclear material by any means of transport.
central control room	A facility from which the function of a Nuclear Power Station is managed and controlled. The facility may also be referred to as the Main Control Room.

TERM	DEFINITION
characterisation	Determination of the nature of the radioactive material and associated evidence.
civil nuclear premises	A civil nuclear site on which NM is used or stored and premises within a nuclear licensed site, in which for example, a person who is not the licence holder, e.g. a tenant that uses or stores NM/ORM. A nuclear premises also includes other locations where Category I, II or III material is used or stored but excludes premises used for temporary storage during approved transportation. It also can be a civil nuclear construction site on which works are being carried out: (i) by a developer; and (ii) pursuant to the grant or issue of a relevant consent, without which the carrying out of those works would be unlawful.
clearance	A generic term used to refer to screening of the workforce that includes both pre-employment checks and national security vetting.
competent authority	A governmental organization or institution that has been designated by the State to carry out one or more nuclear security functions.
compromise	The accidental or deliberate violation of confidentiality, loss of integrity, or loss of availability of an information object.
containment	Structural elements (cans, gloveboxes, storage cabinets, rooms, vaults, etc.), which are used to establish the physical integrity of an area or items and to maintain the continuity of knowledge of nuclear material.
contractor	Company which undertakes work under a contract awarded to it by a civil nuclear company or site licensee. The term includes both Main Contractor and Sub-Contractors.
control (of nuclear material)	Activities, devices, systems and procedures that ensure that the continuity of knowledge (e.g. location, quantitative measurements) about nuclear material is maintained.
criminal or [intentional] unauthorised acts	A general term encompassing malicious acts and any other intentional acts or omissions contrary to UK law or regulations and having nuclear security implications.
cyber security	The collection of tools, policies, security concepts, security safeguards, guidelines, risk management

TERM	DEFINITION
	approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. This is synonymous with the term Computer Security used by the IAEA.
defence in depth	The combination of multiple layers of defence, including both administrative aspects (procedures, instructions, sanctions, access control rules, confidentiality rules) and technical aspects (multiple layers of protection together with measures for detection and delay) that an adversary would have to overcome or circumvent to achieve their objective.
design basis threat	The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal or sabotage, against which a physical protection system is designed and evaluated. The Nuclear Industries Malicious Capabilities Planning Assumptions is the UK's DBT.
detection	A process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorised act and that is completed with the assessment of the cause of the alarm.
detection system	Integrated set of detection measures including capabilities and resources necessary for detection of a criminal act or an unauthorised act with nuclear security implications.
dispersal (direct or release)	Dispersal or release of material by application of energy from an external source (for example, an explosive or incendiary device) on the material.
dispersal (indirect dispersal or release)	Dispersal or release of material by utilizing the potential energy (i.e. heat or pressure) contained in the nuclear or radioactive material or in a process system to disperse the material.
dutyholder	A generic term to describe 'a responsible person', 'approved carriers' and 'relevant personnel' as defined in NISR.
employee	A person directly employed by the licensee of the nuclear site.
force-on-force exercise	A performance test of the physical protection system that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the

TERM	DEFINITION
	threat or the design basis threat
graded approach	The application of physical protection measures proportional to the potential consequences of a malicious act.
guard	A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.
head of security	A person appointed by the Board of the body holding the nuclear site licences to be accountable to it for advising management on the effective implementation of security measures and for monitoring compliance with relevant policies. May also be known as the Company Security Manager.
head of site	A senior manager appointed by the body holding the nuclear site licence who has management accountability for security on the licensed site and (where appropriate) for ensuring that arrangements are compatible and consistent with other parts of any jointly occupied site. The appointment may also be described as Site Director, Station Director or Station Manager.
improvised nuclear device	A device incorporating radioactive materials designed to result in the formation of a nuclear-yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a nuclear weapon.
information security	The preservation of the confidentiality, integrity and availability of information.
initiating event	An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. [Also a maliciously initiated initiating event - a malicious act that upsets the operation in such a way that, if mitigation were unsuccessful, would lead to unacceptable radiological consequences.
inner area	An area with additional protection measures inside a protected area, where Category I nuclear material is used and/or stored.
insider	An individual with authorised access to nuclear facilities or nuclear activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorised acts involving or directed at nuclear

TERM	DEFINITION
	material, other radioactive material, associated facilities or associated activities or other acts determined to have an adverse impact on nuclear security.
integrity	The property of protecting the accuracy and completeness of assets (including information).
international transport	The carriage of a consignment of NM by any means of transportation intended to go beyond the territory of the State where the shipment originates beginning with the departure from a facility of the consignor in that State and ending with the arrival at the facility of the consignee within the State of ultimate destination.
likelihood	The product of threat and vulnerability
limited access area	Designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes.
local police	This term is used to describe any non-CNC police force that has a role to play in the procetion of NM/ORM and may include Home Office, Police Scotland and BTP forces.
main control room	A facility from which the function of a NPS is managed and controlled. The facility may also be referred to as the CCR.
need to know	A principle under which users, processes and systems are granted access to only the information, capabilities and assets which are necessary for execution of their authorised functions.
nuclear material	Material listed in the table on the categorization of nuclear material, including the material listed in its footnotes, in Section 4 of IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).
nuclear security	The prevention and detection of and response to, theft, sabotage, unauthorised access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.
nuclear security event	An event that has potential or actual implications for nuclear security that must be addressed.
nuclear security regime	Nuclear security systems and nuclear security

TERM	DEFINITION
	measures at the facility level, transport level and activity level for detection of, and response to, nuclear security events.
nuclear security system	An integrated set of nuclear security measures.
operator	The licensee within the meaning of section 26(1) of the Nuclear Installations Act 1965.
performance testing	Testing of the physical protection measures and the physical protection system to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements.
physical barrier	A fence, wall or similar impediment which provides access delay and complements access control.
physical protection	Measures (including structural, technical and administrative protective measures) taken to prevent an adversary from achieving an undesirable consequence (such as radiological sabotage, or unauthorised removal of nuclear or other radioactive material in use, storage or transport) and to mitigate or minimise the consequences if the adversary initiates such a malicious act.
physical protection measures	The personnel, procedures and equipment that constitute a physical protection system.
physical protection system	An integrated set of physical protection measures intended to prevent the completion of a malicious act.
protected area	Area inside a limited access area containing Category I or II nuclear material and/or sabotage targets surrounded by a physical barrier with additional physical protection measures.
radiation exposure device	A device with radioactive material designed to intentionally expose members of the public to radiation.
radioactive material	Nuclear material, as defined in the CPPNM; radioactive sources, as defined in the Code of Conduct for the Safety and Security of Radioactive Sources and other radioactive substances containing nuclides which undergo spontaneous disintegration (a process accompanied by the emission of one or more types of ionizing radiation, such as alpha and beta particles,

TERM	DEFINITION
	neutrons and gamma rays).
radioactive source	Radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It also means any radioactive material released if the radioactive source is leaking or broken, but does not mean material encapsulated for disposal, or nuclear material within the nuclear fuel cycles of research and power reactors.
radiological dispersal device	A device to spread radioactive material using conventional explosives or other means.
regulatory authority	Any form of institutional control applied to nuclear material or other radioactive material, associated facilities, or associated activities by any competent authority as required by the legislative and regulatory provisions related to safety, security, or nuclear materials safeguards. Explanation: The phrase 'out of regulatory control' is used to describe a situation where nuclear or other radioactive material is present in sufficient quantity that it should be under regulatory control, but control is absent, either because controls have failed for some reason, or they never existed.
response forces	Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorised removal or an act of sabotage.
response level	The level of security required to be in force at sites in response to the currently assessed threat of terrorist action. The Government uses a three level system (NORMAL, HEIGHTENED AND EXCEPTIONAL) to articulate the Response Level in force across the Civil Nuclear Industry.
risk	The potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences
sabotage	Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.
security by design	A concept where the requirements to provide security for any new facility or modification to an existing facility are considered during all phases of the design and procurement process in parallel with safety needs.

TERM	DEFINITION
security classifications	OFFICIAL, SECRET and TOP SECRET are standard terms used to convey the appropriate levels of protection required for SNI and assets.
security contingency plan	A part of the security plan or a stand-alone document that identifies reasonably foreseeable security events, provides initial planned actions, (including alerting appropriate authorities) and assigns responsibilities to appropriate operator personnel and response personnel.
security force	A component body, formed of the CNC, directly employed civilian guards, or employees of an approved commercial security contractor, which is responsible for operating a security control room, patrolling or controlling access to a site and providing an initial response or an armed intervention to counter an attempted unauthorised removal of NM/ORM or an act of sabotage.
security regime	The security standards, security procedures and security arrangements set out in the approved security plan and applied by the operator for the protection of the site and of any plant, equipment or NM or ORM thereon, or NM in transit.
sensitive information assets	Any equipment or components that are used to store, process, control or transmit sensitive information. For example, sensitive information assets include control systems, networks, information systems and any other electronic or physical media
sensitive nuclear information	Information relating to, or capable of use in connection with, the enrichment of uranium, or information of a description for the time being specified in a notice under section 71 of the Energy Act 2013.
site	A civil site or establishment in respect of which a nuclear site license has been granted, or other nuclear premises containing Category I, II or III Nuclear Material.
sponsor	An authorised individual who is responsible for initiating an application for National Security Vetting.
super sponsor	An individual within an organisation who has the ability to oversee applications on NSVS initiated by all sponsors within their organisation.

TERM	DEFINITION
supply chain	Companies and any subcontracting companies providing services to the dutyholder
target identification	The process of inventory analysis and vital area identification in order to determine a site or facility's categorisation for theft or sabotage.
tenant	Company or its employees who lease premises on a site.
threat	The product of adversary motivation, intent and capability.
threat assessment	An evaluation of the threats, based on available intelligence and open source information, that describes the motivation, intentions, and capabilities of these threats.
threat beyond the DBT	A threat identified in the assessment that, while not included in the DBT, remains credible. Threats beyond the DBT need to be taken into account to ensure the physical protection of nuclear facilities.
two-person rule	A procedure that requires at least two authorised and knowledgeable persons to be present to verify that activities involving nuclear material and nuclear facilities are authorised in order to detect access or actions that are unauthorised.
unauthorised removal	The theft or other unlawful taking of radioactive material or sources.
vetting authority	A function performed by ONR in addition to its regulatory purpose, where it is the decision maker on the suitability of personnel to hold, or continue to hold a national security vetting clearance
vital area	An area containing NM/ORM (including radioactive sources), or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT, could directly or indirectly result in unacceptable radiological consequences, thereby endangering public health and safety by exposure to radiation.

TERM	DEFINITION
vulnerability	A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat, or, weakness of an asset or control that can be exploited by a threat.
vulnerability assessment	A process which evaluates and documents the features and effectiveness of the overall security system at a particular target.
workforce	The people engaged in, or available for work within the UK's civil nuclear industry which includes staff, the supply chain and any subcontractors.

7 ABBREVIATIONS

BPC&I	Basic Process Control & Instrumentation Systems
BPSS	Baseline Personnel Security Standard
BSI	British Standards Institute
BTP	British Transport Police
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security Systems
CCF	Common Cause Failure
CCR	Central Control Room
CNC	Civil Nuclear Constabulary
CNPA	Civil Nuclear Police Authority
CNS	Civil Nuclear Security
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security & Information Assurance
CTC	Counter Terrorist Check
CPS	Cyber Protection System
DAPSyP	Duly Authorised Person for Security Purposes
DBEIS	Department for Business Energy and Industrial Strategy
DBT	Design Basis Threat
DV	Developed Vetting

EEA	European Economic Area
EIMT	Examination, Inspection, Maintenance & Testing
EP&R	Emergency Preparedness & Response
ETUK	Enrichment Technolocy UK
FSyP	Fundamental Security Principle
GDA	Generic Design Assessment
HCVA	High Consequence Vital Area
HEU	High Enriched Uranium
HMG	Her Majesty’s Government
HR	Human Resources
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ICO	Information Commisioners Office
ICT	Information and Communications Technology
ILW	Intermediate Level Waste
IND	Improvised Nuclear Device
ISO	International Standards Oganisation
JTAC	Joint Terrorism Analysis Centre
KSyPP	Key Security Plan Principle
LEU	Low Enriched Uranium
LLW	Low Level Waste
LO	Learning Objective
MFES	Manual Forced Entry Standard

NATO	North Atlantic Teaty Organisation
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations (2003)
NM	Nuclear Material
NMAC	Nuclear Material Accountancy and Control
NSS	Nuclear Security Series
NSV	National Security Vetting
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
PPS	Physical Protection System
RASyP	Regulatory Assessment of Security Plans
RSP	Relevant Statutory Provision
SAPs	Safety Assessment Principles
SC	Security Check
SCM	Supply Chain Management
SIRO	Senior Information Risk Officer
SLA	Service Level Agreement
SME	Subject Matter Expert
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified & Experienced
SyAPs	Security Assessment Principles

SyDP	Security Delivery Principle
TA	Threat Actor
TAG	Technical Assessment Guide
TEA	The Energy Act (2013)
TSS	Transport Security Statement
VA	Vital Area

8 REFERENCES

While every effort has been made to ensure the accuracy of the references listed in this publication, their future availability cannot be guaranteed.

1 The Energy Act 2013
http://www.legislation.gov.uk/ukpga/2013/32/pdfs/ukpga_20130032_en.pdf

2 The Nuclear Industries Security Regulations - Statutory Instrument 2003 No. 403
http://www.legislation.gov.uk/uksi/2003/403/pdfs/uksi_20030403_en.pdf

3 The Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations – Statutory Instrument 2009 No. 1348
http://www.legislation.gov.uk/uksi/2009/1348/pdfs/uksi_20091348_en.pdf

4 The Nuclear Installations Act 1965
http://www.legislation.gov.uk/ukpga/1965/57/pdfs/ukpga_19650057_en.pdf

5 The Nuclear Safeguards Act 2000
http://www.legislation.gov.uk/ukpga/1965/57/pdfs/ukpga_19650057_en.pdf

6 ONR - Purpose and Scope of Permissioning
http://www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf

7 IAEA - The Convention on the Phycisal Protection of Nuclear Material
http://www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf

8 IAEA - Amendment to The Convention on the Phycisal Protection of Nuclear Material
https://www.iaea.org/sites/default/files/infcirc274r1m1.pdf

9 The Nuclear Industries Security (Fees) Regulations 2003 - Statutory Instrument 2005 No. 1654 http://www.legislation.gov.uk/uksi/2005/1654/pdfs/uksi_20051654_en.pdf

10 Government Security Group Government Functional Standard GovS 007: Security.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf

11 The Radiation (Emergency Preparedness and Information) Regulations 2001
http://www.legislation.gov.uk/uksi/2001/2975/pdfs/uksi_20012975_en.pdf

12 ONR - Safety Assessment Principles for Nuclear Facilities
http://www.onr.org.uk/saps/saps2014.pdf

13 IAEA - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

14 CPNI - Guide to Producing Operational Requirements for Security Measures
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

15 ONR - Classifcation Policy for the Civil Nuclear Industry
http://www.onr.org.uk/documents/classification-policy.pdf

16 ONR – Enforcement Policy Statement
http://www.onr.org.uk/documents/2014/enforcement-policy-statement.pdf

17 IAEA - Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment Or Technology (INFCIRC/254)
https://www.iaea.org/sites/default/files/infcirc254.pdf

18 ONR - Nuclear Transport Security Guidance for Approved Class B Carriers Nuclear Transport Security Guidance for Class B Approved Carriers (onr.org.uk)

Further information

This document is available web-only at: http://www.onr.org.uk/syaps/index.htm

Any enquiries regarding this publication should be addressed to:

ONR communications team
Office for Nuclear Regulation
Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS
Email: onr@onr.gov.uk

Published 11/21

Further information about ONR is available at www.onr.org.uk