Managing Changes to Security Standards, Procedures and Arrangements

Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-11.4.6	**Issue No.:**	1
Record Reference:	2022/018929		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Principal Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	First Edition		

Table of Contents

1. Introduction

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

2. The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR 2003') [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This TAG is such a guide.

2. Purpose and Scope

3. This TAG contains guidance to advise and inform ONR inspectors when exercising their regulatory judgment during assessment activities which relate to a dutyholder's processes for managing changes to security Standards, Procedures and Arrangements (SPA) that form the approved security plan. It aims to provide general advice and guidance to ONR inspectors on how this security aspect should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the SPA are adequate.

4. In the context of this TAG, SPA include processes and procedures in addition to security related equipment and infrastructure, together with security staffing arrangements. It is, therefore, akin to the guidance ONR has issued in respect of Licence Condition 22 and Licence Condition 36. These cover modification or experiment on existing plant and changes to organisational capability respectively. Consequently, civil nuclear licensed sites will already have these processes established and may wish to adopt them in order to manage change to their approved Security Plan. Where this is the case, inspectors should satisfy themselves that these arrangements suitably integrate and adequately incorporate security specific aspects. Other dutyholders may wish to adopt similar arrangements as appropriate.

5. Changes to the SPA as referenced in this TAG are defined as:

- Any alteration to buildings, plant, Security Structures, Systems and Components (SySSCs), operations or processes that could potentially affect the security claims and arguments made in the approved security plan if inadequately conceived or executed and, therefore, delivery of the Physical Protection Systems (PPS) outcomes described therein.

- Any change to the organisational structure, staffing level and competencies, including any change to security posts covered in the Nuclear Baseline (NB), or equivalent, through which the dutyholder demonstrates these are, and remain, suitable and sufficient to manage nuclear security and achieve the PPS outcomes described in the security plan. The NB, or equivalent, provides the basis against which any proposed organisational change can be assessed.

- Any change to documents that provide supporting claims, arguments and evidence to justify the security plan and outcomes it describes.

3. Relationship to Relevant UK Legislation and Policy

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

7. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

8. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Key Security Plan Principle (KSyPP) 6 – Managing Changes to Security Standards, Procedures and Arrangements. This TAG is consistent with other TAGs, associated guidance and policy documents.

9. The Government Functional Standard on security [3] describes expectations about 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). As such it is considered Relevant Good Practice (RGP).
The security outcomes and requirements detailed in the Government Functional Standard have been incorporated within the SyAPs. This ensures dutyholders are presented with a coherent set of expectations for the protection of nuclear premises (and SNI), and the employment of appropriate personnel security controls, both on and off nuclear premises.

10. ONR’s Classification Policy [4], which provides guidance on the application of NISR 2003, indicates those categories of SNI, which require protection and the level of security classification that should be applied.

11. A dutyholder may choose to develop security-specific change management processes or adapt their existing safety procedures for this purpose. In any event, the dutyholder should be able to understand the security significance

of the function being performed (this may be through a categorisation and classification process as per KSyPP 5 or similar) and so classify the proposal according to the potential impact if inadequately conceived or executed. This is important in ensuring there is adequate scrutiny and challenge in developing any proposed change to their extant SPA so they will continue to deliver the security outcomes described in their approved security plan. A dutyholder's change management processes should recognise the potential impact, and therefore consequence, of a change in safety or security arrangements (e.g., operations and storage) and the impact that each might have on the other. Therefore, inspectors should draw from guidance both within and outside of the security programme area when considering the effectiveness of a dutyholder's security processes. TAGs of relevance are:

- CNS-TAST-GD-2.1 - Maintenance of a Robust Security Culture [5].
- NS-INSP-GD-022 – LC22: Modification or Experiment on Existing Plant [6].
- NS- INSP-GD-048 – LC 36 Organisational Change [7].
- NS-TAST-GD-080 - Challenge Culture, Independent Challenge, Capability and provision of Nuclear Safety Advice [8].
- NS-TAST-GD-065 – Function and Content of the Nuclear Baseline [9].
- NS-TAST-GD-049 - Nuclear Safety Technical Assessment Guide Licensee Core Safety and Intelligent Customer Capabilities [10].
- NS-TAST-GD-079 - Licensee Design Authority Capability [11].
- NS-TAST-GD-061 – Staffing Levels and Task Organisation [12].

4. Relationship to International Standards and Guidance

12. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [13] and the IAEA Nuclear Security Fundamentals – NSS 20 [14]. Fundamental Principle J of the CPPNM refers to quality assurance and states that a quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.

13. Essential Element 9 of NSS 20 recognises the need for the use of risk informed approaches, not least as these should underpin an effective change management process. It states that an effective nuclear security regime uses risk informed approaches, including the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth, which take in to account the following:

    a) The State's current assessment of the nuclear security threats, both internal and external;

    b) The relative attractiveness and vulnerability of identified targets to nuclear security threats;

    c) Characteristics of the nuclear material, other radioactive material, associated facilities and associated activities;

    d) Potential harmful consequences from criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, associated facilities, associated activities, sensitive information or sensitive information assets, and other acts determined by the State to have an adverse impact on nuclear security.

14. A more detailed description of the elements is provided in Recommendations-level guidance, specifically NSS 13 [15], . It states that operators, shippers and carriers (i.e., dutyholders) should establish sustainability programmes for their physical protection system. It also states that these sustainability programmes should encompass configuration management, which it describes as the process of identifying and documenting the characteristics of a facility's physical protection system (including computer systems and software) and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation.

5. Advice to Inspectors

5.1. The Nature and Purpose of Managing Changes to Security Standards, Procedures and Arrangements

15. SPAs that form an approved security plan may require amendment to reflect updated codes and standards, operational changes on a site, planned works, revised inventory, operational experience, changes to threat etc. To comply with NISR 2003 Regulations 6 and 7, ONR must approve such change before the dutyholder implements it, unless notification to the contrary is provided by ONR under NISR 2003 Regulation 7(2) and/or 8(2). However, not every proposed change will necessarily require formal assessment, and this depends on the associated risk together with its potential impact or consequence. Therefore, dutyholders may wish to develop procedures that enable them to determine the potential impact and consequence of any change prior to submitting a change proposal to ONR. ONR can then focus regulatory activity where it is most needed and avoid unnecessary delay and burden for dutyholders when making minor changes to their SPA, particularly where they do not increase the security risk or invalidate claims made in their security plan. The ability to effectively manage change to security SPA requires dutyholders to not just have appropriately comprehensive and robust processes in place but to underpin these with a strong security culture [5].

6. Regulatory Expectation

16. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies their process for managing changes to SPA that ensures any associated risks are identified and appropriate control measures implemented.

Key Security Plan Principles	Managing Change 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.		

7. Managing Change to Security Standards, Procedures and Arrangements

17. To demonstrate adequate control of changes to the security 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 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 security plan.

18. Change can be temporary or permanent and result from factors including site operations, movement or change in inventory, changes/updates to the organisational structure, staffing or competences 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 SQEP for their role;
- be owned and embedded throughout the organisation, up to and including the board, executive team or equivalent senior management;
- reference the nuclear baseline 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, 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,

- be subject to periodic review on the effectiveness of the overall arrangements and the changes that have been implemented.

19. The intention of KSyPP 6 is to enable dutyholders to develop arrangements for managing changes to their extant security plan, under NISR 2003 Regulations 6 and 7, by demonstrating adequate control of changes to the plan based on their security significance. Accordingly, a dutyholder’s change management processes should include an assessment of the security significance of any proposed change, to determine the most appropriate level of regulatory oversight required before being implemented.

20. As KSyPP 6 is aimed at managing change in respect of NISR 2003 Regulations 6 and 7 it has limited application for approved carriers. However, the principles could be used to develop a process for managing change to transport security statements and associated transport security plans.

21. Changes might be proposed for physical or cyber security arrangements, organisational resources, management systems or document updates including:

- Any alteration to buildings, plants, operations, processes, procedural changes or security case, including replacement, refurbishment or repairs to existing buildings, plants or processes and alterations to the design of plants during the period of construction. Including workarounds, changes/updates to site services.

- Changes to computer-based systems or software.

- Changes to the organisation, number, deployment or working hours of security personnel.

22. Such changes may be:

- **Permanent** – change to some aspect(s) of the extant security SPA due to, for example, an inventory change that necessitates revised storage arrangements, a change to the site layout, revised security categorisation of the site etc. The proposed change could be permanent or long-term.

- **Temporary Security Arrangement (TSA)** – extant SPA may require a TSA to take account of non-physical changes; for example, to the searching and escorting required to facilitate an outage or defueling. ONR expects temporary changes to be time bounded.

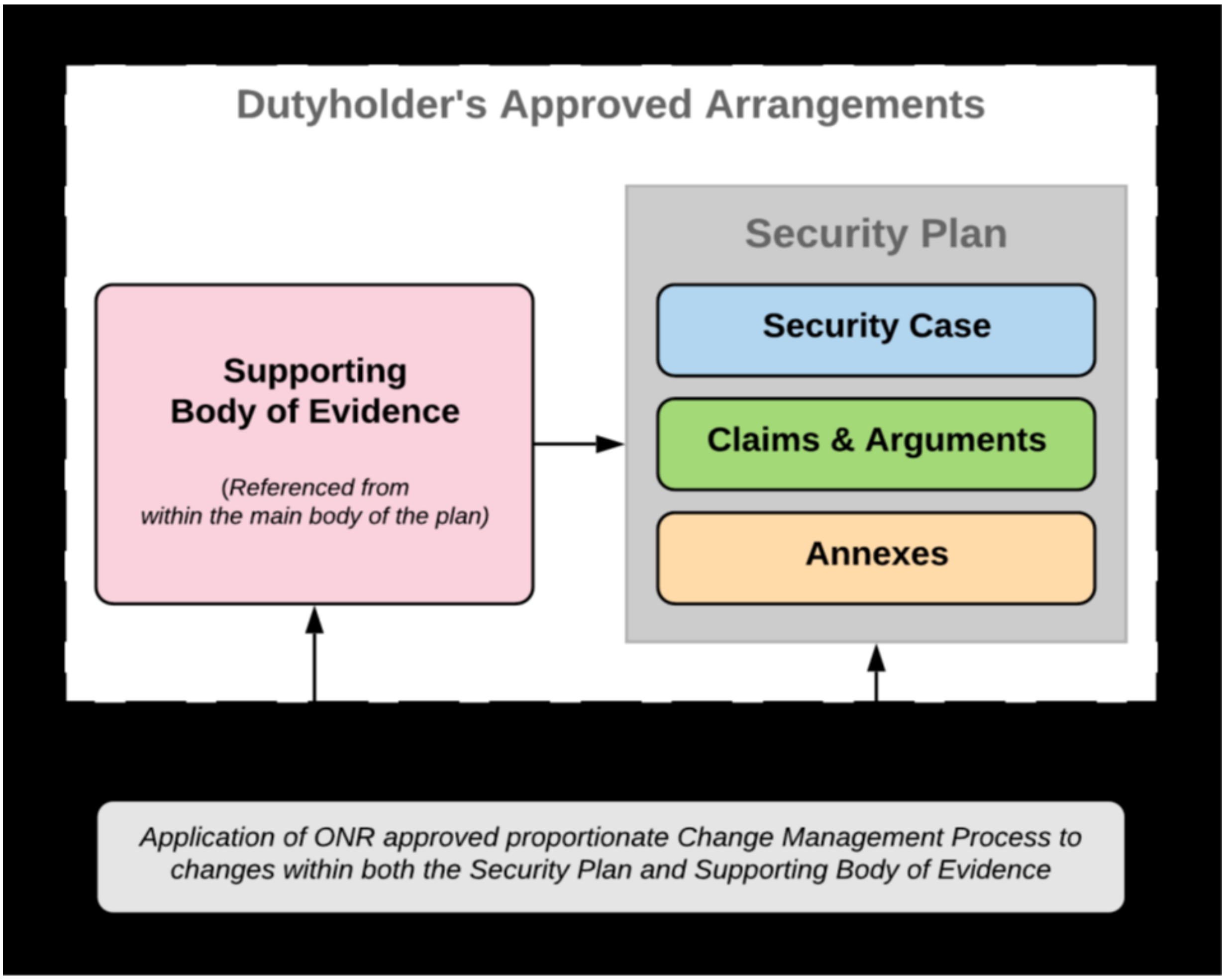
- **Temporary Security Plan (TSP)** – the dutyholder must carry out work that falls under NISR 2003 Regulation 8 (i.e., alteration or extension to any building or structure that is, or forms part of a nuclear premises). A TSP should be time bounded and may result in an associated requirement to permanently amend the SPA once work is complete.

23. It is important a dutyholder’s processes determine the scope and significance of a proposed change in addition to its likely duration. The dutyholder should specify how long they expect a TSA or TSP to be in place. Where work is likely to last for more than 12 months, a permanent amendment to the approved security plan should always be considered. ONR may re-approve any TSA or TSP that, for whatever reason, is not closed within twelve months but the dutyholder should not assume this will happen without their providing further justification.

24. When managing changes to SPA, dutyholders should understand the importance of the security functions affected by a change. That understanding may be demonstrated through use of a categorisation and classification process, or some other robust and effective means. Doing so enables a dutyholder to identify the significance of a change and the security impact or consequence associated with it. Additionally, it ensures the on-going security risk is adequately and appropriately managed through the provision of security mitigation throughout the change lifecycle from design to operations. Inspectors should remember that security SPA may well be supported by, or linked to, a number of other functions on nuclear premises. Thus, change management may be a multi-disciplinary exercise, which requires discussion and interaction between various functions and subject matter experts.

25. A diagram giving an example of the constituent elements of a security plan is provided below. Any proposed change to the SPA must take account of the outcomes an approved security plan describes to ensure these are still delivered and the necessary effect is achieved. It is possible that apparently relatively minor changes to the approved SPA could have a profound effect on the ability of a dutyholder to deliver the effects described in the plan. For example, the exchange or replacement of apparently like-for-like SySSCs may greatly increase risk throughout the project and/or result in an enduring risk thereafter if inadequately conceived or executed. Therefore, to ensure any proposal has been properly graded and that subsequent assessment/approval can be conducted, ONR must be confident those responsible for proposing a change, determining its effects and then delivering it, are sufficiently SQEP and supported by a robust organisation.

26. As stated earlier, the regulatory expectation placed upon dutyholders is that they will ensure the security plan identifies clearly how they manage changes to SPA that form the approved security plan. They will include robust security assurance arrangements and an adequately resourced challenge function. It should also describe the annual review process that ensures 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.


Dutyholder's Approved Arrangements
Security Plan
Security Case
Claims & Arguments
Annexes
Supporting Body of Evidence
(Referenced from within the main body of the plan)
Application of ONR approved proportionate Change Management Process to changes within both the Security Plan and Supporting Body of Evidence

Note: Security plan characteristics are described in RASyP 4 of SyAPs

27. Inspectors should note the effectiveness of a dutyholder’s processes for managing changes to SPA is reliant on them having a complete and thorough understanding of the SPA within the approved security plan and their relative importance in delivering the required outcomes.
Inspectors should also be aware that a dutyholder may already have comprehensive and appropriate Management of Change (MoC) arrangements for operational and organisational change to comply with LC22 and LC36. Whilst these may be extended to manage changes to security SPA, provided internal application and governance is supported by embedded security SQEPs, these arrangements must provide for the legal requirement that ONR approves any change that affects SPA covered in the security plan (unless ONR has provided a notification under NISR 2003 Regulation 7(2) or 8(2)) and accommodates the ONR assessment needed to support regulatory decision making.

7.1. ONR Approval of Dutyholder Processes for Managing Changes to Security Standards, Procedures and Arrangements

28. As alluded to earlier, where dutyholders adopt arrangements to manage changes to SPA and ONR is confident in their efficacy, ONR will be able to issue notifications under Regulation 7 and 8. These notifications will have the effect of allowing dutyholders to implement certain changes without recourse to ONR for assessment, thus reducing regulatory burden. Furthermore, the process will indicate to ONR the significance of the change, allowing it to target regulatory resource on those changes that could result in the greatest consequences if inadequately conceived or executed. The table below provides an illustration of how ONR will adopt a more proportionate approach to assessment and approval of changes to SPA.

29. A diagram to illustrate this is given below.

Category	Regulation	DR1*	ONR Approve	Assessment	Report[1]
MAJOR	6 (1) Permanent 6 (1) TSA 8 (1)TSP	Yes	Yes	Yes	PAR
SIGNIFICANT	6 (1) Permanent 6 (1) TSA 8 (1)TSP	Yes	Yes	Yes – Sampled case-by-case based on confidence in a dutyholder’s processes and Regulatory Intelligence	PAR or DR2 dependent upon complexity and potential hazard
MINOR	6 (1) Permanent 6 (1) TSA[2] 8 (1) TSP	Yes – When sampled	Yes	Yes – When sampled	DR2 – When sampled

[1] PAR and DR2 are ONR internal process
[2] All TSAs require ONR approval as they cannot be covered by NISR 2003 Regulation 7(2) and 8(2) notifications

Category	Regulation	DR1*	ONR Approve	Assessment	Report[1]
NEGLIGIBLE[3]	6(1) Permanent 8(1) TSP	No	Permission under Regulation 7(2) or 8(2) Notifications	Not Routinely	None

30. It must be emphasised that a dutyholder is under no legal obligation to implement such a regime. However, the opportunity to realise the regulatory efficiencies identified within this document will be unavailable should suitable processes not be developed, and inspector's ability to effectively target their assessment activity to changes of higher risk will be reduced. Furthermore, a prescriptive Regulation 8(2) notification will be required to address the issue of all works of physical alteration or extension having to be submitted to ONR for approval.

31. The importance of correctly recognising the significance of a proposed change to SPA cannot be overemphasised. A change that could result in a MAJOR reduction in nuclear security standards and a resultant increase in the risk of a security-initiated event, if inadequately conceived or executed, will require formal assessment and approval by ONR. Similarly, if the proposed change could affect claims and arguments in the approved security plan to such an extent that outcomes may no longer be delivered as described, the plan will require formal assessment and re-approval by ONR. SIGNIFICANT changes that do not affect delivery of the described outcomes might be approved without further assessment if ONR has confidence in the processes that support the change submission; the maturity of the dutyholder; and the dutyholder's capability to assess the impact or consequence of their intended change(s).

32. A change that will have a MINOR effect on nuclear security standards will be submitted to ONR for approval, who will adopt a proportionate level of sampling and assessment. Changes that have 'no effect' will be covered under a Regulation 7(2) notification and consequently there is no legal requirement for them to be submitted to ONR for approval. However, the dutyholder will be expected to record these changes for sampling by its internal assurance function and ONR as required.

33. NISR 2003 requires certain SPA to be in the security plan such as how premises are to be policed and guarded and for the investigation and assessment of relevant personnel. ONR requires that any proposed change to such SPA is formally approved. Dutyholders' security change management processes should take this into account.

[3] Where a proposed change has no security affect or is unlikely to prejudice security

8. Principles for Managing Change to Standards, Procedures and Arrangements

34. Some broad principles underpin ONR’s expectations regarding a dutyholder’s processes for managing change to SPA. These are set out below and each is covered in more detail in the following sections.

8.1. Principle 1

35. **A dutyholder’s processes for managing change to SPA 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.**

36. Dutyholders should have formal, systematic processes in place to assess, monitor and review changes to the approved security plan, thus ensuring they are managed in a co-ordinated, consistent and effective manner, and the risks associated with any proposed changes are properly assessed and controlled. A dutyholder must be able to demonstrate any change will not affect their ability to meet the appropriate PPS outcomes.

37. Processes for managing changes to SPA should be part of the dutyholder’s management systems. Where necessary, they should include the providers of security services (e.g. the CNC or CGF) to ensure all aspects of security delivery are considered as part of the change process. Relevant internal departments/functions (for example, Human Resources, Operations, Human Factors, Occupational Health, etc.) should also be included in these processes, to ensure all implications of a proposed change are considered. The processes should set out the roles and responsibilities for managing change, with clearly assigned responsibilities for initiating, peer reviewing, internal approval levels, monitoring, closeout and post-implementation review.

38. The impact and associated security risk of a proposed change should be assessed using a consistent methodology which focuses on delivery of relevant PPS outcomes. The methodology should be applied to all proposed changes in order to make and record an early judgement of the potential impact on nuclear security. In particular, the security risk, and the potential inability to deliver relevant PPS outcomes (should the change be inadequately conceived or executed), must be determined.

39. Staff, whether the dutyholder’s employees or contractors, involved in all aspects of managing changes to SPA should be SQEP for their role, with SQEP requirements clearly defined.

40. The process should consider and, where possible, allow for the reversal of changes or application of contingency plans, if performance monitoring of a change indicates it has been inappropriately conceived or inadequately implemented. The importance of being able to do so may reflect the significance of the change and the availability of effective countermeasures.

41. All proposed changes to SPA should be subject to a proportionate level of scrutiny and challenge. Thus, the greater the significance of a proposed change, the greater the scrutiny and challenge applied. If appropriate, this might be provided by the Nuclear Safety Committee (NSC) or its equivalent for nuclear security activity.

42. If there is no need for further approval by ONR once the change has been implemented, a SQEP should formally sign off to confirm the intended outcome has been achieved.

43. Dutyholders should monitor the effectiveness of their procedures for managing change to SPA as part of their routine assurance processes.

The inspector should consider

- Are the dutyholder’s processes for managing changes adequately articulated or referenced in the approved security plan?
- Does the dutyholder have formal, documented processes for managing change to their security SPA? (These should be an integral part of their management system)
- Is it clear the processes apply to all aspects of a dutyholder’s activities that have the potential to affect nuclear security and are applied throughout their organisation?
- Are the documented processes clear, available to end users and up to date?
- Do the processes use a methodology that is easy to understand and follow?
- Is the methodology being consistently interpreted and applied?
- Are roles and responsibilities for managing changes to SPA clearly defined and understood by all staff who are responsible for their implementation?
- Are SQEP requirements for staff fulfilling key roles within the change management process clearly defined?
- Are staff fulfilling key responsibilities for managing change to SPA demonstrably SQEP for such roles and have appropriate authority to discharge their responsibilities?

- Are processes for managing changes to SPA subject to and include independent review and audit?

8.2. Principle 2

44. **The board/executive of the dutyholder should own and support the processes for managing changes to SPA and ensure they are embedded throughout the organisation.**

45. A dutyholder's processes for managing change to the SPA should be peer reviewed and implemented consistently and effectively. A visible commitment to these arrangements should be made by the dutyholder's board/executive. The board/executive should be able to demonstrate it uses these processes by regularly reinforcing to the workforce the importance of having and following a robust change process.

46. The board/executive should ensure SQEP resources are in place to develop and implement the management of change to SPA. The board/executive should also oversee the use of those SQEP resources, to include provision for suitable levels of challenge and independent peer review of change proposals as part of the dutyholder's corporate governance arrangements, (including seeking advice from a NSC, or equivalent).

47. Managing change processes for the SPA should apply throughout the organisation, up to and including the executive team and board, noting that strategic and complex changes to the structure or staff composition of a business, or operational focus, often originate at this level.

48. Progress with, and the effectiveness of, the implementation of significant, complex changes should be regularly monitored by the board/executive. It should establish an oversight process for this purpose.

49. The dutyholder's board/executive should proactively discuss significant, complex changes with ONR at an early stage. This will allow the dutyholder to share its intentions with ONR and for ONR to provide advice and guidance as appropriate to support enabling regulation. It will also help ONR to understand the dutyholder's business drivers and to schedule and prioritise its own resources.

50. The board/executive should satisfy itself that managing change processes for SPA are embedded throughout the organisation and there is suitable provision to periodically review the effectiveness of the processes, and to monitor the ongoing health of the dutyholder organisation. It should ensure the reasons for, and progress with, significant, complex changes are communicated to the workforce.

The inspector should consider

- Is the board/executive able to demonstrate their commitment to effectively managing change to SPA?
- Does the board/executive regularly satisfy itself that the managing change processes for SPA are adequate and being implemented effectively?
- Is there a governance process that ensures appropriate oversight of, and challenge to, all proposed changes?
- Is the board/executive involved in assessing the implications of changes that may have a greater potential impact on nuclear security as part of the dutyholder’s governance arrangements?
- Is the board/executive aware of the need to discuss more significant, complex changes with ONR at an early stage?
- Do the dutyholder’s governance arrangements provide for an oversight process to monitor implementation and provide strategic guidance and support for more significant changes?
- Does the board/executive seek regular assurance that implementation of more significant and complex changes is proceeding satisfactorily?
- Does the dutyholder communicate the reasons for, and progress with, implementation of significant changes to the workforce?

8.3. Principle 3

51. **A dutyholder’s arrangements should include a description and justification (baseline) of its organisational structure, procedures and technology necessary for site security.**

52. To meet the expectations expressed in the FSyP the security plan should as appropriate demonstrate the dutyholder has and maintains a suitable and sufficient organisational structure, plus procedures and technology to deliver site security at all times throughout the range of their activities, all of which should be described and justified in the security plan. To demonstrate adequate configuration control, the organisational structure, procedures and technology should be represented in a format that is easily accessible and be a reference point or ‘baseline’ against which the dutyholder can assess the potential impact upon site security of proposed organisational, procedural and technical changes. This ‘baseline’ should be a dynamic document and be routinely updated to ensure it remains current. Therefore, the security plan should describe the components of dutyholder’s security organisation at a level that allows the dutyholder to readily identify these elements and understand the relative contribution they make to security to help assess how they might be impacted by a proposed change.

53. It is noted civil nuclear licensed sites use their NBs as reference points for organisational structure: one for procedures; the management system, and one for safety systems; the asset management system. Together, with the safety case, these form the basis for plant and organisational configuration control. Regulatory expectations for the derivation and content of the organisational NB are provided in Ref 10 and amplified in Refs 11, 12 and 15. Whilst none of these documents explicitly cover security, much of the guidance is applicable as security is a key enabler for safe operations. The key principles from Refs 10, 13 and 14 are provided in Appendices 2 - 5. Inspectors could refer to the full TAGs when undertaking assessment/ inspection of these topics; these documents also indicate where specialist ONR resource is required /advised. Dutyholders may determine how they represent their reference point, but ONR recognises the concept of the NB and associated expectations as good practice.

54. The NB, or an equivalent process, presents and justifies the organisational resources required to deliver activities with the potential to impact upon nuclear security and, therefore, the overarching nuclear safety of a site. Thus, it covers those activities with a positive impact and those which, if inadequately conceived or executed, could lead to an immediate or latent (direct but not immediate) detriment to nuclear security/safety. This includes, for example, the governance of nuclear security, Intelligent Customer capability, Design Authority and drafting of security related documents, as well as frontline work. Again, dutyholders may determine how to achieve this, but ONR recognises the NB and associated expectations as good practice.

55. Security functions provided by the CNC personnel for example, might not be represented on the NB as the dutyholder has no direct control over their activity. However, the dutyholder is required under NISR 2003 to demonstrate that the CNC and guard force complement, and their deployment is, and remains, sufficient to deliver the relevant outcome, and this must be included in the security plan. Similarly, certain emergency response and contractor roles may be referenced rather than included in the NB. Nevertheless, the dutyholder should apply change control arrangements to proposed changes to the providers of security services (e.g., the CNC or guard force) to ensure all aspects of security delivery are considered as part of the change process.

56. Where a NB exists, it should be used as an integral part of the dutyholder's resourcing processes. Dutyholders may wish, therefore, to develop an organisational baseline to support normal business processes. However, dutyholders must clearly articulate the baseline for nuclear security whether in the security plan itself or referenced by the plan and the process for managing changes to it.

57. Dutyholders may wish to have one integrated process for managing changes to safety and security. Where this is the case, dutyholders should include the involvement of suitable SQEPs into the assessment and governance processes to ensure that implications are identified and adequately

controlled. In addition, they need to accommodate interaction between the various purposes within ONR to ensure legal obligations and regulatory requirements are met.

The inspector should consider

- Has the dutyholder documented their organisational structure, procedures and physical protection systems in a readily accessible format to act as 'baseline' for configuration control?
- Do managing change processes include a reference to this baseline and identify whether or not the proposed changes affect baseline roles, procedures or systems?
- Is the baseline regularly reviewed to ensure it is up to date and incorporates changes affecting baseline roles, procedures or systems?
- Do managing change processes for the SPA take account of the cumulative effects of low category changes on the NB?
- Do managing change processes for the SPA take account of baseline vulnerabilities when completing the risk assessment of the change? Are they subject to SQEP challenge and review?
- Are managing change processes for the SPA integrated with human resource/design/engineering processes?
- Is there evidence that the resource implications of proposed organisational changes are shared with human resources as part of the change assessment process?
- Are actions arising from individual changes to the SPA management of change closed and, if not, that unresolved actions are being managed?
- Whilst a dutyholder may have comprehensive and appropriate MoC arrangements for the NB under LC 36/LC22, do these accommodate the legal requirement under NISR 2003 for ONR to approve any change, other than those that have no effect, to SPA covered in the security plan?

8.4. Principle 4

58. **A dutyholder's processes for managing changes to SPA should include an initial screening assessment, which will identify the potential security significance of a proposed change, thus helping to categorise it and establish appropriate internal justification and challenge levels.**

59. It is important that any proposed change is assessed at an early stage to ensure associated security impact or consequence is fully understood. Dutyholders' processes for managing changes to SPA should include an

initial screening assessment to identify the potential nuclear security significance of the proposal (in the event that the change is inadequately conceived or executed). The dutyholder should use this screening to determine the significance of the change and, in turn, the level of analysis, justification and scrutiny applied to a particular change proposal (prior to its submission for regulatory approval and, if necessary, assessment).

60. The significance should be determined by a reasonably conservative understanding of the impact on security outcomes or consequences if the change is inadequately conceived or executed. Potential compensatory measures should not be taken into account at this stage. However, it may be appropriate for credit to be taken for other layers of the existing defence in depth providing these are independent and unaffected by the change when in their normal configuration. Conversely, where there is limited defence in depth and security resource, a relatively minor change at a dutyholder's site may have a profound effect on their ability to deliver the required PPS and so be considered significant in terms of assessment and approval. Thus, the impact of the change on the ability of the PPS (in its totality) to deliver the required outcomes, in combination with the categorisation for theft and sabotage of the site or facility affected are the key factors for determining significance.

61. The categorisation of the security function and classification of the SySSCs required to deliver that function, should help determine the security impact associated with the change and the consequence of it being inadequately conceived or executed. ONR expects the significance of all changes to be independently assessed and challenged, prior to receiving a change or amendment proposal.

62. ONR requires sufficient time to assess and approve any change.
A dutyholder's processes for managing changes to SPA should take account of ONR's need for time to complete relevant assessment and approval work. Where a significant or complex change is planned, there should be early engagement with ONR. Doing so will allow ONR to provide advice and guidance in advance of a change proposal being submitted for approval, and so provide confidence that a dutyholder's approach to determining the security risk associated with a change - and the plans for mitigating it - are likely to meet regulatory expectation.

63. Some proposed changes may be borderline between two categories or classifications. In these situations, ONR expects the dutyholder to take a conservative position and consider the change at the higher level.

The inspector should consider

- Has an initial screening assessment been prepared to identify the potential nuclear security significance of the proposal and to categorise it accordingly?

- Are proposals supported by a clear, consistent and well-informed approach that identifies potential risks throughout the lifecycle of the change?
- Is the classification methodology easy to understand and being applied objectively and consistently throughout the dutyholder's organisation?
- Are there adequate safeguards to ensure under-categorisation of change and/or dividing complex changes into distinct elements (commonly known as 'salami-slicing') do not prevent the totality of changes being fully considered?
- Is there an oversight function to confirm changes have been correctly categorised and challenged, where appropriate, by a SQEP?
- Do the dutyholder's change processes enable timely engagement with ONR?

8.5. Principle 5

64. **A dutyholder's processes for managing changes to SPA should include an initial screening assessment, which will identify the potential security significance of a proposed change, thus helping to categorise it and establish appropriate internal justification and challenge levels.**

65. It is important that any proposed change is assessed at an early stage to ensure associated security impact or consequence is fully understood. Dutyholders' processes for managing changes to SPA should include an initial screening assessment to identify the potential nuclear security significance of the proposal (in the event that the change is inadequately conceived or executed). The dutyholder should use this screening to determine the significance of the change and, in turn, the level of analysis, justification and scrutiny applied to a particular change proposal (prior to its submission for regulatory approval and, if necessary, assessment).

66. The significance should be determined by a reasonably conservative understanding of the impact on security outcomes or consequences if the change is inadequately conceived or executed. Potential compensatory measures should not be taken into account at this stage. However, it may be appropriate for credit to be taken for other layers of the existing defence in depth providing these are independent and unaffected by the change when in their normal configuration. Conversely, where there is limited defence in depth and security resource, a relatively minor change at a dutyholder's site may have a profound effect on their ability to deliver the required PPS and so be considered significant in terms of assessment and approval. Thus, the impact of the change on the ability of the PPS (in its totality) to deliver the required outcomes, in combination with the categorisation for theft and sabotage of the site or facility affected are the key factors for determining significance.

67. The categorisation of the security function and classification of the SySSCs required to deliver that function, should help determine the security impact associated with the change and the consequence of it being inadequately conceived or executed. ONR expects the significance of all changes to be independently assessed and challenged, prior to receiving a change or amendment proposal.

68. ONR requires sufficient time to assess and approve any change.
A dutyholder's processes for managing changes to SPA should take account of ONR's need for time to complete relevant assessment and approval work. Where a significant or complex change is planned, there should be early engagement with ONR. Doing so will allow ONR to provide advice and guidance in advance of a change proposal being submitted for approval, and so provide confidence that a dutyholder's approach to determining the security risk associated with a change - and the plans for mitigating it - are likely to meet regulatory expectation.

69. Some proposed changes may be borderline between two categories or classifications. In these situations, ONR expects the dutyholder to take a conservative position and consider the change at the higher level.

The inspector should consider

- Has an initial screening assessment been prepared to identify the potential nuclear security significance of the proposal and to categorise it accordingly?
- Are proposals supported by a clear, consistent and well-informed approach that identifies potential risks throughout the lifecycle of the change?
- Is the classification methodology easy to understand and being applied objectively and consistently throughout the dutyholder's organisation?
- Are there adequate safeguards to ensure under-categorisation of change and/or dividing complex changes into distinct elements (commonly known as 'salami-slicing') do not prevent the totality of changes being fully considered?
- Is there an oversight function to confirm changes have been correctly categorised and challenged, where appropriate, by a SQEP?
- Do the dutyholder's change processes enable timely engagement with ONR?

8.6. Principle 6

70. **The dutyholder should periodically review the effectiveness of the overall arrangements and the changes that have been implemented.**

71. The dutyholder should be encouraged to capture learning gained from applying its change management process, especially to larger and more complex changes. This should be reflected, as appropriate, in changes to the process (e.g., roles and responsibilities). The process should be subject to periodic review to confirm it is effective and to identify process improvements. Reviews may take the form of formal audit by a dutyholder's assurance function or management reviews as part of a structured approach to business improvement. It may also be necessary for ONR to formally re-assess the adequacy of the change management processes on the basis of regulatory intelligence.

72. It is important that senior management is engaged in the review process to demonstrate leadership and commitment to the change management arrangements. The totality of changes and their impact on the security regime should be regularly reviewed to ensure arrangements are working satisfactorily and that security delivery is not being degraded as a result of a succession of changes, especially if ill-conceived or executed. This holistic, high-level review is also important to ensure that the configuration of SPA on the ground is accurately reflected in the approved security plan.

The inspector should consider

- Is there a post-change review process to enable learning points from successful and unsuccessful changes to be taken into account for future changes and, if appropriate, incorporated into the dutyholder's management of change arrangements?

- Do the arrangements enable the board/executive to monitor the effectiveness of implementation of more significant changes?

- Is there a formal review process to confirm the change management processes are operating satisfactorily?

- Is senior management engaged in the review process and its leadership and commitment demonstrated to the workforce?

- Does the review process involve persons other than those with a specified change management process role to ensure, for example, the views of originators and implementers are captured?

- Is the outcome of reviews shared with the workforce?

- Is there a mechanism for sharing learning and building that learning back into the arrangements as part of continuous improvement?

- Are the cumulative effects of multiple changes on the organisation considered by senior management and is there evidence action is taken to avoid the potential degradation of the dutyholder nuclear security regime?

- Are there measures in place to ensure that the configuration of SPA on the ground continues to be accurately reflected in the approved security plan?

9. Temporary or Permanent Unplanned Changes to Security Standards, Procedures and Arrangements

73. Dutyholders should have arrangements to manage unplanned changes to SPA due to urgent or emergency situations that may affect nuclear security. These changes may be temporary or permanent. Where the change is temporary, arrangements should cater for returning the SPA to pre-modification status. In any case, the arrangements must provide for an appropriate security justification; control over the modification; and include a process to allow for rapid review, assessment and independent verification.

74. Dutyholders' arrangements should demonstrate suitable operational decision-making, including identifying roles, responsibilities and designations to initiate, approve, perform and remove unplanned modifications.
These should be clearly defined, including the need to interface with ONR to ensure any change or reporting complies with NISR 2003. A temporary or unplanned change may also require ONR's formal approval to ensure ongoing compliance with NISR 2003.

75. Where an unplanned change is made, the change management process should include a requirement for their periodic review to confirm:

- whether it is still needed;
- whether it enables delivery of appropriate PPS outcomes;
- whether it has an effect on the approved security plan; and,
- whether the change should become permanent.

10. Applications to Change Security Standards, Procedures and Arrangements

76. Applications to change SPA should contain sufficient information for ONR to understand the proposal, its significance in terms of risk/consequence and whether ONR assessment may be necessary. Applications should include such drawings or photographs as are necessary to illustrate the proposal, if the dutyholder believes they are likely to help an inspector understand what is being proposed. Dutyholders should also take certain other factors into account when preparing a change submission for ONR. These are:

- **Intelligible** – An application, together with whatever documentation and evidence supports it, should be intelligible and structured logically to meet the needs of those who will use it. All references and supporting information should be clearly identified and be easily accessible.

- **Complete** - An application contains the necessary information to show the proposed change will adequately mitigate any security risk created by the proposal and that the dutyholder will continue to meet relevant PPS outcomes, as described in the approved security plan.

- **Evidence Based** – Claims and arguments presented in an application should be supported by evidence that is verifiable and appropriately documented.

- **Robust** - An application should be appropriately robust and be based on recognised security practice and principles.

- **Balanced** – An application should be balanced and appropriately conservative. Any areas of possible uncertainty should be identified in addition to strengths and benefits.

- **Time bounded** – If the change is temporary in nature (i.e., a TSP), it should be time bound.

References

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

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

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

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

[5] ONR, “CNS-TAST-GD-2.1 - Maintenance of a Robust Security Culture”.

[6] ONR, “NS-INSP-GD-022 - LC22 Modification or Experiment on Existing Plant”.

[7] ONR, “NS-INSP-GD-048 - LC36 Organisational Capability”.

[8] ONR, “NS-TAST-GD-080 - Nuclear Safety Advice and Challenge (2020/265933)”.

[9] ONR, “NS-TAST-GD-065 - Function and Content of the Nuclear Baseline”.

[10] ONR, “NS-TAST-GD-049 - Licensee Use of Contractors and Intelligent Customer Capability”.

[11] ONR, “NS-TAST-GD-079 - Licensee Design Authority Capability (2020/265908)”.

[12] ONR, “NS-TAST-GD-061 - Staffing Levels and task organisation (2020/127012)”.

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

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

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

Glossary and Abbreviations

CGF	Civilian Guard Force
CNC	Civil Nuclear Constabulary
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
HCVA	High Consequence Vital Area
HMG	Her Majesty’s Government
IAEA	International Atomic Energy Agency
KSyPP	Key Security Plan Principle
MoC	Management of Change
NB	Nuclear Baseline
NISR	Nuclear Industries Security Regulations
NSC	Nuclear Safety Committee
NSS	IAEA Nuclear Security Series
ONR	Office for Nuclear Regulation
PCR	Police Control Room
PPS	Physical Protection System
SNI	Sensitive Nuclear Information
SPA	Standards, Procedures and Arrangements
SQEP	Suitably Qualified and Experienced Person
SSCR	Site Security Control Room
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
SySSCs	Security Systems, Structures and Components
TAG	Technical Assessment Guide
TSA	Temporary Security Arrangement
TSP	Temporary Security Plan

Appendix 1: Guidance to Inspectors Security Impact Assessment

1. A possible approach dutyholders may consider when developing their arrangements for managing change to security SPA is given below. However, dutyholders are encouraged to develop and adopt arrangements that are suitable for their business and operational needs. Accordingly, any approach will be determined by the way in which the security plan is written, the actual SPA described and the robustness of a dutyholder's security change management processes. Dutyholders should be encouraged to have appropriately robust internal governance procedures to determine the importance of any proposed change, to confirm and provide evidence of the effect on the PPS outcomes and claims and arguments contained in the approved security plan. Also, that any changes are properly categorised, and their execution will be adequately managed.

2. Under the approach below, all MAJOR, SIGNIFICANT and MINOR changes to the security plan will be submitted to ONR for approval in accordance with Regulation 6. Additionally, a similar approach is adopted for TSPs, whereby those graded MAJOR, Significant and MINOR will also be submitted for approval in accordance with NISR 2003 Regulation 8. However, ONR will apply a proportionate approach to assessment and approval based on the identified significance. Furthermore, those changes and TSPs considered to have NEGLIGIBLE effect will be approved through notification under Regulations 7(2) and 8(2), as appropriate, without the need for ONR approval.

Major

3. Changes that are considered to be 'MAJOR' could result in a major reduction in nuclear security standards and a resultant major increase in the impact or consequence of a security-initiated event, if inadequately conceived or executed, and may have a major effect on the claims and arguments given in the approved security plan. MAJOR changes are characterised by the potential to fundamentally alter the security solutions adopted and/or their performance; the supporting claims and arguments; or amend documents that similarly effect standards and/or operating rules such that outcomes cannot be met. 'MAJOR' changes will necessitate thorough analysis and internal assessment by the dutyholder followed by formal ONR assessment.

4. Any change which, if inadequately conceived or executed, might lead to a serious increase in the potential for NM/ORM to be stolen from a site or facility, or a successful act of sabotage through an inability to meet relevant PPS outcomes.

5. Wide ranging company or site changes that have the potential to affect the validity of, or basis on which, the security plan was approved by ONR.

6. Changes which affect the whole of the dutyholder's security function.

7. Inspectors should note the following indicative changes that are likely to have a MAJOR effect on nuclear security:

- Changes in the number of CNC response officers or guards on each shift.
- Large-scale downsizing or outsourcing of a nuclear security significant function.
- Changes to organisational structure, staffing or competences, whether or not included on the NB, that could result in a major reduction in the effectiveness of the nuclear security regime described in the approved security plan.
- Changes to physical security arrangements that affect several levels of defence in depth or/or significantly reduce the security effect of the remaining defence in depth.
- Proposals affecting the security functions such that achievement of relevant outcomes cannot be assured.
- Changes to pre-employment screening and national security vetting levels.
- Changes that may result in complete loss of Site Security Control Room/Police Control Room (SSCR/PCR) functionality.
- Fundamental changes to documentation that underpins the security plan such as, categorisation for theft or sabotage and vulnerability assessments.
- Complex changes to high category security functions that protect against high consequence events.
- Complex software or hardware changes to Computer Based Systems Important to Safety and/or Security.

Significant

8. Changes that are considered to be 'SIGNIFICANT' could result in a significant reduction in nuclear security standards and a resultant significant increase on the impact or consequence of a security-initiated event, if inadequately conceived or executed, and may have a significant effect on the claims, arguments and evidence given in the approved security plan. SIGNIFICANT changes are characterised by the potential to alter the security solutions adopted and/or its performance; the supporting claims

and arguments; or amend documents that similarly effect standards and/or operating rules such that there is less confidence that outcomes can be met. 'SIGNIFICANT' changes will still require thorough analysis and internal assessment by the dutyholder followed by formal ONR assessment.

9. Any change which, if inadequately conceived or executed, might lead to a significant but less serious increase in the potential for NM/ORM to be stolen from a site or facility, or a successful act of sabotage through an inability to meet relevant PPS outcomes.

10. Company or site changes that have a significant impact on the validity of, or basis on which, the security plan was approved by ONR.

11. Inspectors should note the following indicative changes that are likely to have a SIGNIFICANT effect on nuclear security:

- Changes that might lead to degradation of security features during or post implementation and so compromise but not negate delivery of relevant PPS outcomes.
- Significant changes to the security function establishment level such that resilience rather than response may be affected.
- Changes to organisational structure, staffing or competences, whether included on the NB or not, that could result in a significant reduction in effectiveness of the nuclear security regime described in the approved security plan.
- Changes to security systems and operational controls that protect against significant consequences.
- Software or hardware changes to operational and information technology that support but are not critical to safety and security.
- Changes which have a significant potential to affect adversely the overall emergency response and meeting the response outcome.
- Changes to documents that may have an effect on the claims and evidence that support the security case, but do not significantly alter the basis on which the security plan was approved or the delivery of relevant PPS outcomes.

Minor

12. Changes that fall under MINOR could, if inadequately conceived or executed, result in a minor reduction in nuclear security. These would have minor impact on claims and arguments made in the approved security plan. Dutyholders should subject changes they consider to be minor to a proportionate internal analysis to ensure they have a high degree of

confidence in their assessment. These changes require approval, but not necessarily assessment by ONR.

13. Inspectors should note the following indicative changes that are likely to have a minor effect on nuclear security:

- The change, even if inadequately conceived or executed could not lead to a significant consequence or alter the ability to meet the security outcomes.
- Changes to search methodology or the equipment used that has no effect on the proportion of persons searched or the effectiveness of the search regime.
- Minor changes to SySSCs where significant defence in depth still exists and relevant PPS outcomes are still achieved.
- Minor changes to the required level of security SQEP provided the overall effect is still delivered.

Negligible

14. A change that is considered to be NEGLIGIBLE whereby it is non-prejudicial to nuclear security will be permissioned through the issue of a 7(2) or 8(2) notification as appropriate. Accordingly, they will not need to be submitted to ONR for approval prior to implementation. However, there is still an expectation that dutyholders will subject such changes to suitable analysis to have confidence in their assessment. Furthermore, a record should be maintained by the dutyholder, which may be periodically reviewed by ONR to confirm compliance with the approved arrangements.

Appendix 2: Definitions

15. The following concepts are relevant to the principles outlined in Appendices 3, 4 and 5:

16. **'Core Security Capability'** means the knowledge, functional specialisms and resources that the dutyholder should maintain within its own organisation in order to be able to control and oversee security at all times. This core capability should be a sustainable entity and will include technical, operational and managerial elements. The dutyholder's 'Intelligent Customer' and 'Design Authority' capabilities are sub-sets of the overall core security capability

17. **'Contractor'** means any organisation or individual person that provides a product or service for a dutyholder under a legally binding contract but who is not in the dutyholder's direct employment or formally seconded to from the parent company (which encompasses a Parent Body Organisation). This definition also includes divisions or functions of the parent company organisation appointed by the dutyholder's organisation to provide specific services e.g., Architect Engineer (AE) or Responsible Designer (RD) services.

18. **'Embedded Contractor'** means individuals or members of contractor organisations that are subject to the dutyholder's competency requirements and competency assessments. These personnel are supervised in the same manner as a normal employee. Embedded Contractors can be part of the core security capability and can be acting as an Intelligent Customer.

19. **'Intelligent Customer.** The concept of Intelligent Customer was developed by ONR and has gained international acceptance. It is currently defined by the IAEA4 as follows:

> "An organisation (or individual) that has the competence to specify the scope and standard of a required product or service and subsequently assess whether the supplied product or service meets the specified requirements."

20. ONR considers that the concept of Intelligent Customer relates to the attributes of an organisation rather than the capabilities of individual post holders. ONR defines an Intelligent Customer as –

> "The capability of an organisation to understand where and when work is needed; specify what needs to be done; understand and set suitable standards; supervise and control the work; and review, evaluate and accept the work carried out on its behalf".

[4] IAEA Nuclear Energy Series-No NG-T-3.10-Workforce Planning for New Nuclear Power Programmes

21. Inspectors should be aware that Intelligent Customer roles typically arise in the following areas, although it should be noted that this is not a definitive list:

- security plan production;
- PPS design and engineering;
- IT management in relation to design, installation or maintenance;
- Procurement and supply chain management;
- Projects;
- Site construction/commissioning;
- SySSCs – operations and maintenance.

22. This guidance may also be used to inform ONR assessment of the procurement of security critical equipment which will be manufactured to the specification of the dutyholder, or others formally appointed to act on its behalf.

Appendix 3: Key Principles for the Function and Content of the Organisational Nuclear Security Baseline

1. The Nuclear Baseline (NB) should consider the delivery and oversight of all activities which have the potential to impact upon nuclear security. This includes activities with a positive impact and those which, if inadequately conceived or executed, could lead to an immediate or latent detriment to nuclear security;

2. The NB should address the requirements of steady state conditions, periods of change and potential emergency situations at the current phase of the site/facility's life cycle;

3. The NB should demonstrate that the dutyholder's organisation has sufficient staff and competencies to discharge its responsibilities for delivery and oversight of nuclear security;

4. The dutyholder must demonstrate that it remains in control of nuclear security. The governance of nuclear security and Intelligent Customer capability are an intrinsic part of this demonstration;

5. Contract staff should appear as part of the NB resource when they are embedded within the dutyholder's organisation or meet the criteria for holding Intelligent Customer roles on behalf of the dutyholder;

6. The dutyholder should have arrangements in place to manage contract staff who do not meet the criteria for inclusion in the NB, and in these cases the NB should include those employees who discharge the associated Intelligent Customer functions;

7. The dutyholder should develop a set of Nuclear Baseline Indicators that provide evidence that the NB has the right organisation, staffing levels and competences and that it is being managed effectively;

8. The dutyholder should have in place a process through which the NB is derived and managed;

9. The NB should be maintained as a living document and provide an accurate, current reference point against which nuclear security implications of proposed modifications to staffing levels/structures, workloads, and changed competence requirements can be identified, evaluated, managed and regulated.

Appendix 4: Key Principles for Core Security and Intelligent Customer Capability

1. The dutyholder should maintain a core security capability of staff to ensure effective control and management for nuclear security;

2. The dutyholder should retain overall responsibility for, and control and oversight of, the nuclear and radiological safety and security of all of its business, including work carried out on its behalf by contractors (note that this is a legal requirement);

3. Dutyholder choices between sourcing work in-house or from contractors should be informed by a company policy that takes into account the nuclear security implications of those choices;

4. The dutyholder should maintain an intelligent customer capability for all work carried out on its behalf by contractors that may impact upon nuclear security;

5. The dutyholder should ensure that it only lets contracts for work with nuclear security significance to contractors with suitable competence, standards, management systems, culture and resources;

6. The dutyholder should ensure that all contractor staff are familiar with the nuclear security implications of their work and interact in a well-co-ordinated manner with its own staff;

7. The dutyholder should ensure that contractors' work is carried out to the required level of security and quality in practice.

Appendix 5: Key Principles for the Design Authority Capability

1. The Design Authority should be a defined function within a dutyholder’s organisation which is independent of operations and has a clearly defined reporting line to the Board of the dutyholder organisation;

2. The Design Authority should have the authority and the responsibility to approve or reject proposed design changes and concessions;

3. The Design Authority should have the capability to understand the totality of the design and security plan in the context of each stage of the full plant lifecycle;

4. The Design Authority should have the resources, capability and management processes to assess changes to the physical protection systems, and have the authority to recommend modification to or suspension of operations;

5. The Design Authority should have appropriate up to date knowledge, skills, experience and resources;

6. The Design Authority should regularly assess and determine the continued adequacy of the security plan and have the authority and responsibility to respond to the issues identified.

7. Where the Design Authority does not have the detailed, specialised knowledge required of all the systems and components important to security it may choose to assign those responsibilities to ‘Responsible Designers’ using the supply chain.