1

ONR GUIDE			
PROCUREMENT AND INTELLIGENT CUSTOMER CAPABILITY			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-4.1 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2024
Approved by:	Matt Sims	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.23373. (2019/135622)		
Revision commentary:	Fit For Purpose Review of Rev 0		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 2).

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

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's supply chain management arrangements. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

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

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers supply chain management to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 3) and the IAEA Nuclear Security Fundamentals (Reference 4). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 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'. The importance of issues relating to assurance activities are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12

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

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

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 4.1 – Procurement and Intelligent Customer Capability, in support of FSyP 4 – Nuclear Supply Chain Management. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 6) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 7) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 This TAG informs regulatory assessment of Supply Chain Management (SCM) arrangements and procurement activities for nuclear security related items or services. It establishes ONR's expectations of the purchaser, as the organisation at the top of the Supply Chain. It considers the procurement of items or services in support of construction, manufacture, repair, replacement, modification of plant and equipment.

6.2 The level of ONR scrutiny is dependent on the security significance of the items or services being procured. This scrutiny might include confirmation of the adequacy of the supplier's quality management arrangements and/or be part of the manufacturing

or construction inspection activities identified via the supplier's quality planning arrangements.

Regulatory Expectations

6.3 The regulatory expectation is that dutyholders will describe in the security plan how they successfully procure items or services for nuclear security and maintain an intelligent customer capability to support their nuclear supply chain management arrangements.

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.		

6.4 In delivering this principle, dutyholders (or purchaser on their behalf) should:

- maintain the capability to recognise work of nuclear security significance to ensure it is subject to appropriate procurement procedures;
- utilise an effective procurement cycle for work with nuclear security significance including the use of Operational Requirements or an equivalent robust methodology;
- establish an effective commercial strategy to enable delivery of the security plan;
- maintain an intelligent customer capability for all work carried out on its behalf by suppliers that may impact upon nuclear security;
- develop appropriate specifications, with appropriate stakeholder input, to support the procurement of items or services (including those relating to cyber security or information assurance) of nuclear security significance;
- ensure appropriate arrangements are in place for all contracts involving security classified information or equipment including that considered SNI in accordance with FSyP 7 and its associated delivery principles; and,
- where the work involves SNI, Issue a Security Aspects Letter, or equivalent, detailing how information should be appropriately security classified and protected.

7. PRINCIPLES AND EXPECTATIONS

7.1 ONR's expectations for the principles to be applied to the procurement of goods and services with nuclear security significance is summarised in Diagram 1 below.

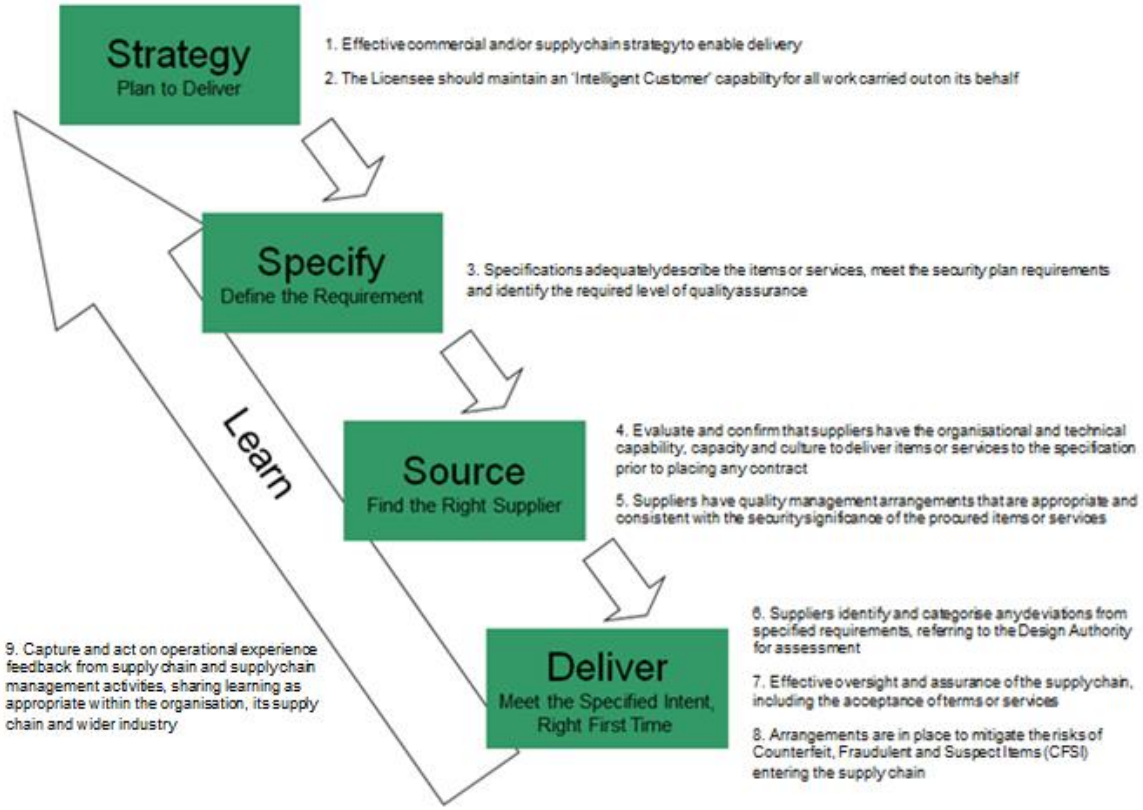

Diagram 1

7.2 The dutyholder should also ensure that suppliers protect all tender documentation, specifications and operational requirements in accordance with their security classification.

8. ESTABLISH AN EFFECTIVE COMMERCIAL AND SUPPLY CHAIN STRATEGY TO ENABLE DELIVERY OF SUCCESSFUL REQUIREMENTS

8.1 The purchaser's commercial and/or Supply Chain strategy will influence all arrangements associated with the procurement of nuclear security related items or services. An effective strategy, deployed through the organisation's business planning process should enable delivery of security plan.

8.2 The purchaser should ensure their commercial and/or Supply Chain strategy addresses current and future security plan provisions over the lifetime of the facility, including decommissioning. Arrangements should be regularly reviewed as they could be effected by various factors including, for example:

- parent body organisation ownership; aggregation of contracts across multiple dutyholders or organisations under parent group ownership, performance
- changes in the Supply Chain; mergers, acquisitions, insolvency, capability and performance

- security of supply; business continuity, strategic/critical suppliers, globalisation of Supply Chains
- make/buy policy; outsourcing and in-house capability or supply
- drive to improve efficiency and competitiveness while enhancing quality and security performance

8.3 The purchaser's commercial and/or Supply Chain strategy, policy and arrangements should be appropriately resourced and include measures to mitigate the risks of any problems in the Supply Chain adversely affecting the security plan. These arrangements should be subject to routine review as part of the organisation's business planning processes to ensure they remain effective and are proportionate to mitigating identified risks.

Inspectors should consider:

- Has the purchaser developed a commercial and/or Supply Chain strategy to address current and future security plan considerations?
- Does the purchaser have effective arrangements to manage their Supply Chain including a clear strategy and/or policy, with roles and responsibilities clearly defined?
- Does the purchaser have the organisational capabilities to manage supply chain delivery?
- Does the purchaser regularly review their SCM arrangements to ensure they continue to support delivery of the security plan?
- Has the Supply Chain strategy been developed using learning available from within the organisation, Supply Chain, nuclear and wider industry?
- Does the strategy encourage collaborative working with the Supply Chain, sharing common security aims, objectives and success criteria?
- Do the purchaser's make/buy (i.e. outsourcing and in-house provision) arrangements effectively consider current and future security plan needs as part of the decision making criteria?

9. EFFECTIVE PROCUREMENT CYCLE – SECURITY SPECIFICATION

9.1 The dutyholder should issue security specifications that adequately describe the items or services, enable delivery of the security plan/achieve operational requirements and identify the required level of quality assurance.

9.2 Establishing an effective security specification is of key importance in the procurement cycle. An ineffective specification will mean that any contractor in the Supply Chain will find it difficult to deliver the purchaser's requirements right first time, regardless of their own capabilities and processes. The dutyholder should also have a process in place to ensure that the supplier is reliable and can provide the equipment or service in an acceptable timeframe.

9.3 Given the importance of the security specification, it is essential that those writing them are Suitably Qualified and Experienced (SQEP) to perform the task and their work is subject to the appropriate levels of internal assurance, including verification, validation and approval, commensurate with the security significance of the item or service being procured. At the pre-contract stage, the purchaser should ensure that prospective suppliers fully understand that the items or services being procured are important to the delivery and maintenance of an effective nuclear security regime.

9.4 The specification should detail applicable design codes and standards that help to fully describe the items or services to be procured together with other generic contractual requirements. This combination of requirements should identify the appropriate levels of quality assurance that are needed. These should include, where applicable, assessment, audit, quality planning, quality control, inspection, surveillance, testing, and release or handover of items, and should fully detail the records package to be supplied with the item or service.

9.5 For items or services which are the principal means of ensuring nuclear security, additional assurance and inspection arrangements may be required, which go beyond basic compliance with established design codes and standards. ONR may wish to assess the technical specification used as the basis for procurement before the process starts, so it is assured that relevant outcomes will be achieved.

9.6 Throughout the design process, the purchaser should conduct appropriate assurance activity to confirm the design meets their requirements, together with applicable codes or standards, and they will continue to deliver the approved security plan in line with regulatory expectations.

9.7 Where a contractor prepares technical specifications for nuclear security significant items or services on behalf of the purchaser, these should be reviewed by SQEP staff from the purchaser's organisation to confirm specifications properly reflect the design intent, meet any design codes and standards, and enable delivery of the security plan. This review should be carried out before contract placement.

9.8 On receipt of the purchase order, the supplier should carry out a review of the contract documentation to ensure it can fulfil all the technical, procedural and commercial requirements of the contract. For complex and high capital value security equipment, discussions between the supplier (and sub-suppliers) and purchaser should normally have covered these aspects prior to contract placement. The supplier should advise the purchaser of any changes to its (or its sub-suppliers) ability to fulfil the contract as such changes arise.

9.9 The purchaser should operate a change control process to ensure any changes to the specification, design or contract are properly controlled and authorised, and the implications for nuclear security and the manufacturing/delivery processes, including changes to documentation (particularly process related - e.g. quality plans), are fully considered prior to the implementation of the change. Where these changes affect the security plan, they may require further assessment by ONR.

Inspectors should consider:

- Do specifications reflect the design intent, design codes and standards, and enable delivery of the security plan?
- Are specifications prepared by contractors reviewed by SQEP staff from the purchaser's organisation?
- Are appropriate levels of quality assurance applied to the procurement of items or services significant to nuclear security?
- Do the purchaser's specification and assurance arrangements address any specific regulatory requirements?
- Do suppliers fully understand that the items or services being procured are a means of ensuring and maintaining nuclear security, and, therefore, their significance?
- Are variations to specification, design or contract properly conceived, communicated, implemented and assessed for their nuclear security implications and then authorised by SQEP purchaser's staff?
- Do suppliers notify the purchaser of any proposed changes who then properly assesses and authorises them?
- Are supplier documents (e.g. quality plans and manufacturing instructions) re-approved before a change is implemented?

10. EFFECTIVE PROCUREMENT CYCLE – DEVIATIONS FROM SPECIFIED REQUIREMENTS

10.1 The purchaser should ensure suppliers identify and categorise any deviations from specified requirements with reference to their Design Authority (DA – as defined in Security TAG 1.2) for assessment. Where any deviations are made the purchaser should ensure these do not affect the proposed security outcome.

10.2 Non-conformances are unplanned deviations from the purchaser's requirements and can be identified in a number of ways including through inspection, audit or surveillance. They can occur at any level within the Supply Chain. Deviations can be associated with an item or service or be the result of the inadequate implementation of the approved process.

10.3 The identification, reporting and resolution of deviations should not be seen as negative, but as an indication that achieving the purchaser's requirements is of prime importance. The control of any deviation from the technical specification is fundamental to the achievement of quality and therefore the integrity of the item.

10.4 All organisations within the Supply Chain should as part of their quality management arrangements operate consistent arrangements, overseen by the purchaser, for the categorisation and disposition of deviations.

10.5 Dutyholders, and purchasers at each level of the Supply Chain should ensure their suppliers have adequate arrangements for the identification, categorisation and management of deviations for items or services. These should include obtaining the approval of the purchaser, or dutyholder's DA, for the deviation in the form of a concession or procedure for re-work. Ultimately they should inform the dutyholder and potentially ONR (via the dutyholder if this is the case) for deviations that are significant to nuclear security.

10.6 Technical Queries (TQs) are slightly different to a non-conformance. For the former, the supplier is asking seeking answers/approval to a question prior to doing the work, while for the latter work has started and is either found to be outside the acceptance criteria for the product, or the process has not been implemented as approved. TQs are raised during the work planning stage and help inform or clarify the contract requirements. Once the purchaser agrees to a TQ that requires a change in the design or other process, the purchaser should track the modification using a formal change control procedure agreed with the supplier if applicable. The purchaser's arrangements should ensure that both types of deviation from the originally specified requirements are appropriately controlled, approved and documented.

10.7 An audit trail should be provided in work control documents for all approved deviations as well as systematic overarching deviation tracking logs that show the status of each deviation. Approved deviations should be incorporated in drawings to reflect 'as built' status to aid configuration control for future modifications.

Inspectors should consider:

- Are deviations identified, characterised and formally sanctioned by competent persons with the appropriate delegated authority?
- Do suppliers bring all deviations of nuclear security significance to the attention of the purchaser, dutyholder's DA and, if appropriate ONR, via the purchaser at the head of the Supply Chain?
- Is there a demonstrable audit trail for all approved deviations from the work control document to logs showing the status of each deviation raised, approved, rejected or reworked with links to required document changes?

11. EFFECTIVE PROCUREMENT CYCLE – COUNTERFEIT FRAUDULENT AND SUSPECT ITEMS (CFSI)

11.1 The purchaser should have arrangements to mitigate the risks of Counterfeit, Fraudulent and Suspect Items (CFSI) entering their Supply Chain.

11.2 There should be recognition throughout all levels of the Supply Chain that there are parties who might wish to substitute CFSI for genuine items or services for commercial gain or with malicious intent. All purchasers should be aware of the risks and hazards of CFSI entering the nuclear industry Supply Chain and understand their role in mitigating this risk.

11.3 The purchaser or supplier should deploy appropriate mitigating measures to prevent CFSI impacting on their Supply Chain depending on the scale, complexity, any

international involvement in and/or nuclear security application of their items or services.

11.4 The following non-exhaustive list presents appropriate mitigation measures that should be deployed as part of a purchaser/supplier's management system, to defend against CFSIs for high risk items or services:

- robust SCM and procurement process arrangements including effective Supply Chain oversight and assurance, including inspection and testing
- competent staff involved in the acquisition processes from specification of requirement through to inspection and receipt of items and services and review of associated records
- material or component traceability back to source supplier, including verification testing by third party specialist organisations for high risk items
- use of positive material identification and destructive testing methods during product inspection, testing and receipt and as part of assurance sampling of high risk proprietary items
- product samples of known precision and authenticity available for comparison with purchased items
- training and awareness within purchasing organisation SCM teams (i.e. Engineering, Procurement, Audit & Inspection), partners and suppliers. Staff should be aware of the risks of CFSI and be trained in mitigation and detection methods as appropriate
- processes and procedures to identify, investigate, record incidences of CFSI and share lessons learnt
- benchmarking with other purchasers
- liaison with Trading Standards and security agencies
- requirements clearly defined in contract terms and conditions
- the effective management of non-conforming items to prevent their re-entry into the Supply Chain as genuine items

11.5 The purchaser should have arrangements in place to quarantine a suspect item or service. Further investigation will be required by the purchaser or supplier to confirm the item as conforming, non-conforming, counterfeit or fraudulent.

11.6 Examples of counterfeit or fraudulent items or services should be shared within the purchaser and/or the dutyholder organisation, Supply Chain and wider industry as appropriate to support learning, prevent use and encourage remedial measures in other impacted facilities, but only when the purchaser has conducted sufficient investigation to confirm if the item is CFSI or not. ONR should be informed of all examples of counterfeit or fraudulent items or services confirmed within the purchaser's Supply Chain that impact on high risk items or services or relate to shortfalls in the purchaser's SCM or procurement arrangements.

Inspectors should consider:

- Does the purchaser have effective processes in place to prevent CFSI entering their Supply Chain at any level?
- Is the purchaser employing positive material identification and effective testing methods during its assurance arrangements, including sample testing of proprietary high risk items?
- Are staff in the purchaser's acquisition processes competent to perform their role and aware of the risks of CFSI, and do they understand and comply with the organisation's mitigation methods?
- Does the purchaser have appropriate arrangements in place to quarantine, investigate and disposition suspect items as conforming, non-conforming, counterfeit or fraudulent?
- Has the purchaser established arrangements to raise awareness of CFSI within their Supply Chain and are they encouraging the open reporting of CFSI examples to maximise learning and mitigate risks?
- Can the purchaser provide examples where they have identified CFSI and taken appropriate remedial measures including notifying ONR and the sharing of learning through their Operational Experience (OPEX) arrangements?

12. EFFECTIVE PROCUREMENT CYCLE – SUPPLY CHAIN OPERATIONAL EXPERIENCE (OPEX)

12.1 The purchaser should have arrangements to capture and act on OPEX feedback from its Supply Chain and SCM activities, sharing learning as appropriate within the organisation, its Supply Chain and wider industry.

12.2 The purchaser should have effective OPEX processes that capture and act upon cross discipline (e.g. engineering, commercial, quality, inspection and test, safety & security etc.) SCM issues associated with the sub-standard procurement of high-risk items or services from specification of requirements, sourcing of suppliers, oversight of delivery, inspection, test and installation or use.

12.3 The purchaser should ensure relevant learning is captured and acted upon from their Supply Chain, related to the provision of high risk items and services. This could include incidences of CFSI in their Supply Chain tiers, sub-standard Supply Chain performance issues that could affect the purchaser at the top of the Supply Chain and factors that might influence future commercial and/or Supply Chain strategy.

12.4 The purchaser should recognise that key suppliers (such as those providing niche products or construction contractors) in the nuclear industry could provide items or services to multiple dutyholders and as such, sub-standard performance from a key industry supplier could affect the nuclear security related activities of multiple dutyholders.

12.5 The purchaser's OPEX processes should enable the wider sharing of relevant Supply Chain and SCM experience with other dutyholders and wider industry as appropriate. Arrangements should be in place to evaluate OPEX shared by other dutyholders, and wider related industry, in case it has implications for the purchaser's organisation and management system arrangements.

12.6 ONR should be informed of confirmed instances of sub-standard Supply Chain performance in the provision of high-risk items or services, particularly where the supplier is likely to form part of the Supply Chains of other or future dutyholders.

Inspectors should consider

- Is the purchaser's OPEX process established, capturing and acting upon sub-standard performance issues associated with their SCM arrangements?
- Is the purchaser's OPEX process capturing and acting upon issues occurring within their different Supply Chain tiers?
- Are OPEX arrangements generating improvements in the purchaser's SCM arrangements and influencing commercial and/or Supply Chain strategy?
- Does the purchaser evaluate relevant learning from other dutyholders, purchasers and supplier organisations, nationally and internationally as appropriate?
- Does the purchaser share learning with its Supply Chain and wider industry as appropriate?

13. MAINTAINING AN INTELLIGENT CUSTOMER CAPABILITY

13.1 The concept of intelligent customer (IC) for safety is defined by the IAEA as follows:

> *'As an intelligent customer, in the context of nuclear safety, the management of the facility should know what is required, should fully understand the need for a contractor's services, should specify requirements, should supervise the work and should technically review the output before, during and after implementation. The concept of intelligent customer relates to the attributes of an organisation rather than the capabilities of individual post holders'.*

This equally applies to nuclear security and a dutyholder's intelligent customer capability for security will be a subset of its core capability.

13.2 Primary responsibility for the security of a nuclear premise rests with the dutyholder who should be able to demonstrate sufficient knowledge of the plant design and security plan for all plant and operations on their site. The dutyholder must be in control of activities on its site, understand the hazards associated with its activities and how to control them, and have sufficient SQEP resource within its organisation to act as an 'Intelligent Customer' for any work it commissions externally.

13.3 In the context of effective SCM the dutyholder should maintain an 'Intelligent Customer' capability to know what is needed, to fully understand the need for a contractor's services, at any level of the Supply Chain, specify requirements, supervise work and technically review the output before, during and after implementation.

13.4 ONR's regulatory expectations of a dutyholder's arrangements for the use of contractors, for retaining control of nuclear security and for discharging its other duties are summarised as follows. The dutyholder should:

- have sufficient SQEP in-house staff to ensure effective control and management for nuclear security
- retain overall responsibility for, and control and oversight of, nuclear security and security of all of its business, including work carried out on its behalf by contractors
- ensure choices between sourcing work in-house or from contractors is informed by a company policy that takes into account the nuclear security implications of the selection
- maintain an Intelligent Customer capability for all work carried out on its behalf by contractors that may impact upon nuclear security;
- ensure that it only lets contracts for work with nuclear security significance to contractors with suitable competence, security standards, management systems, culture and resources
- ensure that all contractor staff are familiar with the nuclear security implications of their work and interact in a well-coordinated manner with its own staff
- ensure that contractors' work is carried out to the necessary level of security and quality in practice

Inspectors should consider:

- Does the dutyholder retain and maintain the core capability to understand, specify, oversee and accept nuclear security related work undertaken on its behalf by contractors at any level of the Supply Chain?

14. REFERENCES

1. **Security Assessment Principles**

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

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

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

5. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

6. **HMG Security Policy Framework**. Cabinet Office. https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

7. **NISR 2003 Classification Policy** – http://www.onr.org.uk/syaps/index.htm

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

15. GLOSSARY AND ABBREVIATIONS

CFSI	Counterfeit, Fraudulent and Suspect Items
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
IC	Intelligent Customer
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
OR	Operational Requirement
SC	Supply Chain
SCM	Supply Chain Management
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
TQ	Technical Query