ONR GUIDE			
OVERSIGHT OF SUPPLIERS OF ITEMS OR SERVICES OF NUCLEAR SECURITY SIGNIFICANCE			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-4.3 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2024
Approved by:	Matt Sims	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19074. (2019/135632)		
Revision commentary:	Fit for Purpose Review of Revision 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 4.3 – Oversight of Suppliers, 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 is to be used by inspectors in their assessment of the adequacy of the dutyholder's arrangements for the supply chain management of items or services of nuclear security significance.

6.2 The effective procurement of items and services is a fundamental element in the provision of an adequate security infrastructure to deliver an appropriate and enduring security effect.

Regulatory Expectations

6.3 The regulatory expectation is that dutyholders will describe in the security plan how they apply oversight of suppliers of items or services of nuclear security significance to support effective nuclear supply chain management arrangements.

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

6.4 The dutyholder (or purchaser on their behalf) should establish an effective commercial and/or Supply Chain strategy to enable effective delivery of items and/or services. The purchaser's commercial and/or Supply Chain strategy will influence all arrangements associated with the procurement security items or services. An effective strategy with appropriate oversight and assurance, deployed through the organisation's business planning process should ensure delivery of an effective security solution.

6.5 Oversight arrangements should include measures to review contracts, how relationships are managed and performance analysis of vendors.

6.6 There are parties who might wish to substitute counterfeit, fraudulent or suspect items (CFSI) for genuine items or services for commercial gain and assurance activities should include a focus on the application of processes to prevent such items from entering the Supply Chain. Of equal concern is that parties may wish to incorporate a 'back door' to Operational Technology or Information Technology (OT/IT) to allow subsequent ease of access following installation. Dutyholders should be aware that such 'back doors' can create significant vulnerabilities and give specific consideration to mitigate their introduction. There is also the possibility that a party acting maliciously may wish to introduce latent defects (for example by installing malware on OT/IT) for subsequent exploitation. Dutyholders and their supply chain should recognise these issues and have in place appropriate arrangements to mitigate them.

6.7 Assurance activities should ensure appropriate arrangements are in place for all contracts involving security classified information or equipment including that considered SNI in accordance with FSyP7 and its associated delivery principles.

7. SUPPLY CHAIN OVERSIGHT AND ASSURANCE

7.1 The dutyholder should conduct effective oversight and assurance of the Supply Chain, including the acceptance of items or services for work with security significance.

7.2 The dutyholder should establish effective arrangements for the oversight of supplier performance throughout the contract period and their quality assurance to ensure that items or services will meet the specified intent. The dutyholder should ensure that it has sufficient capability to oversee and assure performance throughout the tiers of the Supply Chain. Assurance activities should include the inspection, test, release, acceptance and storage of security significant items and services.

7.3 Dutyholders should develop and retain sufficient Intelligent Customer capability to specify, conduct oversight and assurance, monitor manufacturing, fabrication and testing, and acceptance for technical adequacy of the items or services being purchased.

7.4 The dutyholder's oversight and assurance arrangements should review the supplier's security culture and procedures, during and post contract award to ensure the Supply Chain organisations and their leaders continue to understand and promote the importance of nuclear security and the contribution of any security significant equipment or service they supply, to achieving the requirements of the dutyholder.

7.5 The level of oversight and assurance deployed by the dutyholder should be guided by the performance of the supplier or Supply Chain. If performance is below expectation then the dutyholder should increase the level of engagement, oversight and assurance controls until supplier performance meets expectations or until completion or termination of the contract. Conversely, if a supplier demonstrates routine delivery to the specified requirements, right first time, every time, the dutyholder may consider a change to the method and extent of oversight and assurance as appropriate (i.e. from release inspection at the manufacturer's works to receipt inspection at the purchaser's facility).

Oversight

7.6 The level of oversight deployed by the dutyholder should be commensurate with the impact of the item or service if it fails to meet the specified intent. The dutyholder's approach should be influenced by the type of contract, the performance of the supplier, their suppliers and the implications to security of poor performance. Dutyholders are likely to deploy some or all of the following approaches:

- Contract Review – Meetings between the supplier and dutyholder should review performance and delivery issues including security requirements.
- Supplier Relationship Management – Used to maintain effective relationships between the supplier and dutyholder throughout the contract period to achieve common objectives. Effective relationship management should support a collaborative approach between the dutyholder and supplier.
- Vendor Analysis – Performance analysis throughout the contract period with data collated on contract success criteria, delivery to correct quality, specification, schedule and cost. Vendor analysis may be utilised to target and demonstrate improvements, rank and rate suppliers and maintain a dutyholder's preferred suppliers listing.
- Review of the supplier's quality assurance arrangements to ensure appropriate standards are also applied to their suppliers alongside appropriate testing of these items on receipt.

7.7 The dutyholder's Supply Chain oversight arrangements should generate quantitative and qualitative performance data to demonstrate that suppliers of security significant items or services will meet specified target levels. Dutyholders should instigate remedial measures as appropriate, which may include withdrawal of a contract, to address sub-standard performance that may adversely affect nuclear security.

Assurance

7.8 The dutyholder should have suitable assurance and acceptance processes for items or services being supplied or undertaken by others on its behalf. The level of assurance, inspection and test deployed upon item or service completion should be commensurate with the security significance of the item or service being supplied.

7.9 Acceptance of items or services may include verification or independent assessment using second or independent third party organisations. This should be planned and executed, in part, by the application of quality plans. This approach provides essential levels of assurance which are in addition to that provided through the supplier's own quality arrangements.

7.10 In deciding the levels of assurance, in addition to the security significance of the item or service, the dutyholder should consider: the level of assurance normally applied to the item or service for its intended use, the code/standard requirements, and the difficulty of inspection and testing post-manufacture or installation. It is important that ONR has access to all parties that are carrying out quality related activities if requested. Access is normally arranged through the dutyholder. This should include lower-tier suppliers.

7.11 The dutyholder's assurance activities should examine the effectiveness of arrangements for the transport, receipt and storage of items or assembly sub-components within the dutyholder's facilities prior to delivery from the supplier. The storage arrangements should be sufficient to maintain item traceability and prevent damage, loss, deterioration, tampering or inadvertent use.

Inspectors should consider:

- Do the dutyholder's oversight and assurance processes allow them control of their supply chain management and procurement process arrangements for security significant items, from specification of requirement and sourcing a supplier including contract award, through to manufacture of item, construction of facility or provision of item or service?

- Does the dutyholder confirm through its oversight and assurance processes that its expectations are understood, communicated throughout the Supply Chain and routinely reviewed to ensure that suppliers have appropriate understanding of the security application and importance of their high consequence items or services?

- Does the dutyholder have sufficient capability to oversee and assess performance throughout the Supply Chain, and confirm that the level of oversight and assurance deployed by the supplier post contract award is commensurate with the risk of the item or service failing to meet the specified intent? These QA arrangements for the supply chain may be delivered by the principal contractor employed by the dutyholder.

- Does the dutyholder utilise qualitative and quantitative data to demonstrate supplier performance during contract execution and instigate remedial measures where appropriate?

- Is the dutyholder carrying out adequate and appropriate assurance and acceptance of items or services being supplied or undertaken by others on its behalf?

- Are any Inspection Agencies used competent to provide third party assurance and verification of items or services significant to security?

- Do the dutyholder's assurance processes undertake regular reviews of the supplier's quality activities including the release of hold points, with the level of evidence to support hold point release defined and tested?

- Do the dutyholder's assurance processes undertake regular reviews of supplier's quality activities for Technical Queries (TQs), with a specific focus on the aggregation of multiple TQs or those considered security significant?

- Does the dutyholder seek assurance from suppliers that the measures introduced to prevent CSFI from entering supply chain are in place and effective?

8. REFERENCES

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

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://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf

7. **NISR 2003 Classification Policy**

   http://www.onr.org.uk/documents/classification-policy.pdf

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

9. GLOSSARY AND ABBREVIATIONS

CFSI	Counterfeit, Fraudulent or Suspect Item
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
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
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