ONR GUIDE			
SUSTAINABILITY OF NUCLEAR SECURITY ARRANGEMENTS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-5.3 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2022
Approved by:	Matt Sims	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19075. (2019/135650)		
Revision commentary:	Fit for Purpose Review of Rev 0		

TABLE OF CONTENTS

Published 03/20

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 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 arrangements to ensure sustainability of their security regime. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT 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 reliability, resilience and sustainability to be important components 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) and the IAEA Nuclear Security Fundamentals (Reference 3). 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 sustainability is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:

  (a) Developing, implementing, and maintaining appropriate and effective integrated management systems including quality management systems;

  (b) Demonstrating leadership in nuclear security matters at the highest levels;

  (c) Developing, fostering and maintaining a robust *nuclear security culture*;

  (d) Allocating sufficient human, financial and technical resources to carry out the organization's nuclear security responsibilities on a continuing basis using a risk informed approach;

  (e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the *nuclear security systems*;

  (f) Having in place processes for using best practices and lessons learned from experience;

  (g) Establishing and applying measures to minimize the possibility of *insiders* becoming *nuclear security threats*;

  (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 The importance of sustainability is also recognised 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 4). This document states 'Operators, shippers and carriers should establish sustainability programmes for their Physical Protection System (PPS). Sustainability systems should encompass (*inter-alia*):

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair and calibration.
- Performance testing and operational monitoring.

- Configuration management (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).

- Resource allocation and operational cost analysis.

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 5.3 – Sustainability, in support of FSyP 5 – Reliability, Resilience and Sustainability. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) 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 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 For the purposes of this TAG, sustainability is defined by the set of objectives and implementing actions incorporated into the nuclear security regime to support its continuing effectiveness. If the nuclear security regime is to remain effective, it needs to be sustained over time.

6.2 Inspection and assessment activities should be proportionate to the potential consequences of the relevant malicious acts directed at nuclear material, other radioactive material, associated facilities or associated activities, or other acts which may have an adverse impact on nuclear security. The guidance set out in this TAG should be applied taking account of the graded approach.

6.3 At an operational site/facility level, sustainability applies to those nuclear security systems and measures implemented at a facility or in connection with any activity where nuclear or other radioactive material is possessed, produced, used, handled, stored or disposed or where nuclear or other radioactive material is in transport. Sustainability includes:

- Operating procedures (instructions).
- Human resource management and training.

- Equipment updating, maintenance, repair and calibration.
- Performance testing and operational monitoring.
- Configuration management (the process of identifying and documenting the characteristics of a facility's PPS — 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).
- Resource allocation and operational cost analysis.

Regulatory Expectations

6.4 The regulatory expectation placed upon the dutyholder is that the security plan identifies how their arrangements ensure sustainability of the nuclear security regime at their site and/or facilities.

FSYP 4 - Reliability, Resilience and Sustainability	Sustainability	SyDP 5.3
Dutyholders should ensure that the constituent parts of its nuclear security regime are sustained and supported over time to ensure it continues to achieve the required outcomes.		

7. MANAGING AND PLANNING FOR SUSTAINABLE OPERATIONS

7.1 Achieving the objective of effective management and planning at the operational level sustains the nuclear security regime through the continuous allocation of resources to ensure the effective design, operation and maintenance of nuclear security systems and measures.

7.2 Suitably Qualified and Experienced (SQEP) senior managers set priorities and identify the long-term (i.e. duration of risk) financial resources needed for ongoing operational expenses related to personnel, training, exercises, performance testing, procurement, EIMT and replacement of equipment, and for configuration management. Managers also define roles, responsibilities and accountabilities. Dutyholders should document these management decisions in order to achieve the intended objectives.

7.3 Plans enable dutyholders both to demonstrate conformity with applicable requirements and provide guidance to their own personnel for the operation, maintenance and continuous improvement of nuclear security systems and measures. At nuclear premises, SQEP staff prepare the security plan and associated contingency plans. These must be re-evaluated when any relevant change may impact on the objectives being achieved. Similarly, approved carriers of nuclear material prepare transport security statements which are also subject to periodic review and amendment.

7.4 The dutyholder's senior managers should set priorities, identify long-term financial resources, and define roles, responsibilities and accountabilities for nuclear security in order to ensure the continuing effectiveness of the organisation's nuclear security system.

Inspectors should consider:

- Are relevant management decisions documented as part of a formal approval process? (See Security Decision Making TAG (Reference 9).
- Is risk management applied to security related risks, as a comprehensive, robust and ongoing process that is part of a risk informed approach? Risk management includes identification of assets and risks, planning and executing risk reduction actions, assessing the effectiveness of the actions and acceptability of residual risks, and repetition and improvement of the process.

8. IDENTIFYING AND APPLYING CURRENT THREAT INFORMATION

8.1 Achieving the objective of identifying and applying current threat information, enables dutyholders to tailor appropriately the security systems and measures which ensure the effectiveness of their nuclear security regimes.

8.2 Ensuring that nuclear security systems and measures remain effective depends upon periodic review and adjustment of such systems and measures to address updated information on relevant current threats.

8.3 Relevant threat information may be provided through a variety of sources, such as the national threat assessment process, the Design Basis Threat (DBT) (Reference 8), the police and other operators. Dutyholders should establish and maintain regular liaison with such sources.

8.4 Dutyholders should establish a process for ensuring the threat information they receive is systematically and promptly addressed through modifying nuclear security systems and measures as necessary. Dutyholders should also establish mechanisms to address increases in the Response Level.

8.5 Dutyholders should document the process for identifying and addressing current threat information in their security/contingency plans.

Inspectors should consider:

- Does the security plan:
  - Incorporate consideration of appropriate threat information and application of a risk informed approach?
  - Include appropriate agreements and identify relevant external organisations that may need to be contacted or informed in the case of a nuclear security event?
  - Include a process for regular review and revision, based on operational feedback and changes in requirements?
  - Make appropriate arrangements for ongoing measurement and assessment of security performance, and to achieve ongoing improvement?

- Has the dutyholder established and documented a systematic process for exchanging, maintaining and acting on current threat information in a timely manner, including establishing and maintaining relationships with relevant authorities to facilitate information exchange?
- Does the dutyholder review and mitigate potential insider threats through such means as the personnel security programme, information security measures and security training?
- Does the dutyholder adapt nuclear security systems and measures as necessary, to counter the current threat?
- Does the dutyholder implement appropriate compensatory measures in response to a specific, emerging or increased threat?
- Does the dutyholder have a mechanism for reporting updated threat or system effectiveness information to the responsible competent authorities?

9. DEVELOPING AND MAINTAINING NUCLEAR SECURITY COMPETENCES

9.1 The development and maintenance of nuclear security competences at the operational level sustains the nuclear security regime by ensuring the continuing availability of effective, well-motivated, SQEP nuclear security personnel who understand their responsibilities in this regard.

9.2 Sustainability depends on the dutyholder having sufficient staff with the competences necessary for effective operation and maintenance of its nuclear security systems. The dutyholder should establish systems and processes for recruiting qualified staff and/or training staff to attain these competences.

9.3 Recruitment of appropriate staff may be supported by outreach to educational institutions, professional societies and trade associations, as well as the dutyholder's own human resource department.

9.4 The dutyholder should establish programmes for providing the necessary training, either by using internal resources, or through external training providers. These programmes should include specific mechanisms for career development. Sustainable operations benefit from staff who are not only qualified and trained to discharge their responsibilities effectively, but who are also motivated through professional recognition to continue in long-term careers with the dutyholder.

Inspectors should consider:

9.5 Competence management is explicitly covered by FSyP 3. Therefore, where appropriate, inspectors may consider that competence related aspects of sustainability have been addressed where a dutyholder's security plan has been assessed as meeting the regulatory expectations of SyDPs 3.1 to 3.4.

10. ESTABLISHING AND IMPLEMENTING A MAINTENANCE PROGRAMME

10.1 Establishing and implementing effective maintenance programmes at the operational level sustains the nuclear security regime by ensuring that related systems and equipment perform reliably and effectively over time. The dutyholder should be

capable of performing timely maintenance by using its own workforce, contractors or a combination of both.

10.2 Periodic equipment maintenance against an appropriate schedule, including repair, replacement and calibration, is essential to the stable and reliable operation of systems and equipment. It reduces the amount of down time due to equipment failures, and maximises the effective operational lifetime of equipment. Regular, planned system checks and preventive maintenance can optimise performance and provide advance warning of possible system outages or maintenance problems so that timely mitigating actions can be planned and taken. A formal maintenance programme helps ensure malfunctioning system components are promptly identified and repaired, adequate spare parts are available to minimise system outages, and that all equipment is calibrated within expected parameters, according to an established schedule. Maintenance programmes should also provide for compensatory measures when systems are out of service for maintenance.

10.3 Dutyholders should take into account equipment lifecycles, including upgrading or replacing equipment as it fails or becomes obsolete. Conducting equipment upgrades or replacement on a rolling basis may help minimise the financial and operational impacts of maintenance or replacement.

10.4 Assessment of systems to ensure any significant ‘Single Points of Failure’ that might undermine the objectives being achieved, are identified and mitigated where appropriate.

Inspectors should consider:

10.5 Issues concerning maintenance are explicitly covered in the Examination, Inspection, Maintenance and Testing TAG (Reference 10). Therefore, inspectors may consider that maintenance related aspects of sustainability have been addressed where a dutyholder’s security plan has been assessed as meeting the regulatory expectations of SyDP 5.2.

11. APPLYING CONFIGURATION MANAGEMENT

11.1 Configuration management sustains a nuclear security regime by ensuring that information on critical systems and processes is consistent with the physical and operational characteristics of the system and is available in a timely manner to facilitate the making of informed decisions. Also, it ensures that only authorised changes are made to systems in accordance with local control arrangements.

11.2 Configuration management involves documenting the physical, procedural and training elements of an operating organisation’s critical nuclear security systems. It can encompass design documents, standard operating procedures and governing guidelines for the system as well as processes for coordinating changes to the facility’s systems or operations that may adversely impact the effectiveness of nuclear security systems.

11.3 Configuration management ensures that changes to a nuclear security system are properly developed, implemented, verified and documented. Having immediate access to this information can help the operating organisation recover rapidly from hardware or software failures and ensure equipment is operating as intended when returned to service. In addition, access to accurate records regarding training, procedures,

maintenance and logistics allows the dutyholder to verify that these important elements that support a nuclear security system are in place.

Inspectors should consider

- Does the dutyholder apply configuration management to document the physical, procedural and training elements of its critical nuclear security systems?
- Does the dutyholder ensure configuration management information is accurate, available in a timely manner and appropriately protected?
- Does the dutyholder ensure the security implications of changes in the nuclear security systems subject to configuration management are reviewed prior to implementation and are documented appropriately?
- Does the dutyholder ensure the security implications of changes in other systems that have an impact on nuclear security are reviewed prior to implementation and are documented appropriately?
- Does the dutyholder identify critical nuclear security systems in the security plan along with any relevant protection required?

12. PROMOTING ROBUST NUCLEAR SECURITY CULTURE

12.1 Promoting a robust nuclear security culture at the operational level sustains the nuclear security regime by ensuring that dutyholder management and staff understand and appreciate the need to maintain an effective nuclear security regime.

12.2 Nuclear security culture is the assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions that serve as a means to support and enhance nuclear security. A strong nuclear security culture is based on an appreciation and awareness of the threat, that nuclear security is important, and that effective security is everyone's responsibility within the dutyholder organisation including contractors. A robust nuclear security culture, with strong leadership and employee recognition, motivates staff at all levels within the dutyholder to meet their responsibilities, including reliable operation and maintenance of nuclear security systems and measures.

Inspectors should consider:

12.3 Issues relating to organisational culture are explicitly covered by FSyP 2 and specific guidance on assessing nuclear security culture can be found in in the Nuclear Security Culture TAG (Reference 11). Therefore, inspectors may consider that culture related aspects of sustainability have been addressed where a dutyholder's security plan has been assessed as meeting the regulatory expectations of SyDP 2.1.

13. CONDUCTING COMPLIANCE AND PERFORMANCE EVALUATIONS

13.1 Conducting regular compliance and performance evaluations sustains the nuclear security regime by identifying strengths and areas for improvement in nuclear systems and measures. It also confirms that the security regime complies with that described in the extant approved security plan.

13.2 Compliance and performance evaluations help dutyholders identify aspects of their systems that need improvement. Any shortcomings should be recorded, together with the timescale for the implementation of any corrective action, within the Site Security Plan's Security Improvement Schedule (SIS) or equivalent. Depending on the severity of any vulnerability caused by the shortcoming and the time required to complete the corrective action, it may be necessary to implement interim compensatory security measures (possibly through use of a Temporary Security Plan (TSP)) to ensure that risks remain adequately mitigated. The rigour of the evaluation should be based on the graded approach, depending on the nature of the operations as well as the security system and measures.

13.3 Compliance evaluations should be designed to assess the dutyholder's security systems and measures against regulatory requirements.

13.4 Performance evaluations should be designed to assess performance of the dutyholder's systems and measures in meeting applicable performance objectives and addressing the defined nuclear security threats. A significant component of performance evaluation may be performance testing, through both limited scope tests (focusing on an individual component) and system-wide tests of the entire security system. Performance testing should include the investigation, measurement, validation and verification of nuclear security systems and measures against a measurable outcome.

13.5 When compliance and performance evaluations indicate that any element of the security system is deficient or not performing adequately, corrective action, including compensatory measures if required, should be taken to ensure relevant security objectives are still achieved. Where appropriate this should be reported to ONR in accordance with NISR2003 Regulation 10. Compensatory measures (i.e. a TSP) will require approval and possible assessment by ONR. Any corrective action that is not readily achievable may need to be formally recorded in the SIS.

Inspectors should consider

- Does the dutyholder implement formalised and documented compliance and performance evaluations?
- Is the SIS, or equivalent, within the security plan up to date?
- Are shortcomings noted in the SIS addressed by the dutyholder through compensatory measures such as a TSP?
- Does the security plan validate functional requirements and performance of the systems? The plan should provide a basis for the design, frequency and performance criteria for the testing programme. These evaluations should verify that criteria for reliability, operability, readiness and performance are met.
- Does the dutyholder ensure that performance tests and exercises are conducted regularly, including tests and exercises with external response organisations?
- Does the dutyholder document results of evaluations, including corrective actions and, where appropriate, report the results and findings to ONR?

- Does the dutyholder engage with other organisations to share lessons learned and best practices? With respect to both the process of evaluation and results.
- Does the dutyholder ensure that tests are conducted rotationally to verify that all human factor contributions to security sustainability are assessed?

14. REFERENCES

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

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

3. **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

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

5. **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

6. **NISR 2003 Classification Policy** – http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles** – CM9 Ref. 2017/121036

8. **Design Basis Threat**

9. **ONR Security Decision Making** TAG – CM9 Ref. 2019/354886

10. **ONR Examination, Inspection, Maintenance and Testing** TAG –CM9 Ref. 2019/135642

11. **ONR Nuclear Security Culture** TAG – CM9 Ref. 2019/135595

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

15. GLOSSARY AND ABBREVIATIONS

CPPNM	Convention on the Physical Protection of Nuclear Material
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
SIS	Security Improvement Schedule
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide