ONR GUIDE			
EXAMINATION, INSPECTION, MAINTENANCE AND TESTING OF PHYSICAL PROTECTION SYSTEMS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-5.2 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19075. (2016/100358)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/17

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). 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 1).

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 their security systems are subject to an appropriate regime of Examination, Inspection, Maintenance and Testing (EIMT). 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) (Reference 4) 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 quality assurance 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:
    - Developing, implementing and maintaining appropriate and effective integrated management systems including quality management systems.
    - Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear security responsibilities on an ongoing basis using a risk-informed approach.
    - Routinely conducting maintenance, training and evaluation to ensure the effectiveness of the nuclear security systems.
    - 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 quality assurance 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 2). This document states "The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

4.4 Additionally, NSS 13 recognises the importance of sustainability, specifically paragraph 3.57 'Operators, shippers and carriers should establish sustainability programmes for their physical protection system. Sustainability systems should encompass (*inter-alia*):

- Equipment updating, maintenance, repair and calibration; and
- Performance testing and operational monitoring.

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 Security Delivery Principle (SyDP) 5.2 – Examination, Inspection, Maintenance and Testing, 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 Physical Protection Systems (PPS) are designed on the premise that the supporting security equipment infrastructure will achieve the standards of reliability claimed in the security plan, thus ensuring risks are appropriately managed and controlled. The reliability of a protection system will only be assured through the site's full lifecycle by a process of Examination, Inspection, Maintenance and Testing (EIMT) which may include refurbishment or replacement of Security Structures, Systems and Components (SSCs). This process is based upon a sound understanding of the PPS, the identification of SSCs important to security, knowledge of the security equipment's characteristics as it ages and the implementation of an appropriate EIMT programme.

6.2 EIMT activities should be proportionate to the potential consequences of the relevant malicious acts (as detailed in the Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) document (Reference 8)) 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, as described in the SyAPs.

Regulatory Expectations

6.3 The regulatory expectation placed upon the dutyholder is that the security plan identifies the nature and intervals of EIMT for critical elements of the security system and provides appropriate justification for any long term performance claims without EIMT. EIMT activities should take account of any reliability claims in the security plan and be appropriate for the life cycle and/or PPS outcome required of the site.

6.4 There should be traceability of EIMT requirements from the security plans through the Plant Maintenance Schedule to Maintenance Instructions.

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

7. EXAMINATION, INSPECTION, MAINTENANCE AND TESTING THROUGH FACILITY LIFE

7.1 The provisions of EIMT are relevant to the whole life cycle of a nuclear facility. The nature and balance of these provisions, and hence the associated regulatory expectations, change during the various stages of the life cycle.

8. DESIGN AND SECURITY PLAN DEVELOPMENT

8.1 Dutyholders should confirm that the security plan identifies the nature and periodicity of the proposed EIMT and provides a justification for any claims associated with any part of the PPS without an EIMT programme. Whenever the latter claim is made, the inspector should confirm the adequacy of the additional design measures incorporated to justify the absence of EIMT, or the arguments and evidence cited in support of such a claim.

8.2 A key element of the arrangements should be consistency at all stages from the identification of SSCs in the security plan through to the Plant Maintenance Schedule, to the maintenance instructions (which may be termed job plans). This consistency should include the ability to readily identify the SSC classification and security functional requirement for a SSC from anywhere within the chain of documents, e.g. through the use of clear SSC cross-references between documents.

8.3 Inspectors should note dutyholders may produce a Plant Maintenance Schedule that includes other plant. In such instances, the inspector should determine whether anything that may affect nuclear security is clearly identified. A systematic approach to identifying SSCs for inclusion in the Schedule should be adopted.

9. MANUFACTURE AND WORKS TESTS (FACTORY ACCEPTANCE TESTS)

9.1 Relevant works tests should be formally documented and captured in the dutyholder's operational documentation (for example, Quality Plans) as the baseline for ongoing demonstration that the design intent of the protection system for the facility is maintained.

10. ON SITE PLANT INSTALLATION, FACILITY ACCEPTANCE TESTS AND COMMISSIONING (SITE ACCEPTANCE TESTS)

10.1 Plant changes during installation and testing should be adequately assessed in terms of identifying resultant effects on the proposed EIMT arrangements. Such changes may result in the need to modify the Maintenance Schedules and Maintenance Instructions.

10.2 For equipment of particular concern (and where it is not possible for tests to confirm the ability to operate under the most onerous design conditions), the inspector should seek justification of the components' performance and reliability from additional analysis utilising data from commissioning or rig-testing. Reference data should be taken from type-testing to establish a baseline for comparison against in-service performance.

10.3 As a project proceeds, dutyholders should document changes to the Maintenance Schedule and Maintenance Instructions along with records of the consideration and agreement by all relevant project, security, and operations disciplines.

10.4 Dutyholders should consider the extent to which the commissioning will demonstrate the proposed in-service test regime for each part of any such system, as well as the whole system itself.

10.5 Where an EIMT activity to satisfy a security requirement is shown on the appropriate assumptions database, cross references to its security role definition within the nuclear security plan, unique numbers for the test documents, maintenance instruction number and completion sign off for inactive commissioning, should be provided as appropriate.

11. OPERATIONS

11.1 EIMT for the various SSCs should be specified, standards selected and the work undertaken to a level of quality commensurate with their security Classification.

11.2 Attention should be paid to the following security plan concerns:

- Confirmation that any security plan requirements for staggered testing are translated into the Maintenance Schedule.
- Confirmation that, in constructing the Maintenance Schedule, the dutyholder has considered and demonstrated that the minimum configurations of operational security systems justified in the security plan will be maintained.
- Where equipment important to security is taken out of service for EIMT, temporary security plans should be in place to provide commensurate levels of protection or provide adequate mitigation where this is not possible. Furthermore, the potential for the EIMT to initiate a fault or generate a vulnerability, should be analysed and the associated risks appropriately assessed and managed.

12. INSPECTION BASED MAINTENANCE

12.1 Dutyholders should establish that the programme of work provides the necessary EIMT for the PPS (within an overall long term plan) and includes any additional work identified following, or arising, from any specific security concerns identified during operation of the facility.The EIMT programme should be assessed by SQEP personnel from the dutyholder's Operational and Design Authority organisations.

12.2 All EIMT activities should be carried out to written procedures, and that appropriate arrangements are in place for the independent checking (by sampling) of inspections to confirm that appropriate quality is maintained.

12.3 Dutyholder's arrangements for the reporting and reviewing of results, categorisation and sentencing of defects, (including independent assessment where appropriate), should be assessed to confirm overall acceptability.

12.4 Where there is a regulatory or procedural control over restart, all findings which are pertinent to the security justification for the restart should be provided in good time for consideration by inspectors.

12.5 Procedures should be sampled in order to confirm they contain clear and adequate instructions, guidance on reporting criteria and provide adequate means of identifying and recording items inspected and any features or defects observed.

12.6 SQEP staff should review the final outage inspection reports, or any equivalent reports, and advise whether any of the matters reported raise new concerns which should be considered before equipment is brought back into service.

13. VERIFICATION OF EIMT

13.1 The dutyholder should have a process for confirming maintenance has taken place and records any repairs or modifications. It should be graded to reflect the importance of that equipment to nuclear security and associated EIMT. This should specifically include an appropriate level of physical verification of EIMT on the facility.

14. PERIODIC SECURITY REVIEWS

14.1 Periodic reviews of security by both the dutyholder's plant and security directorate(s)/department(s) as part of the overarching internal assurance programme, should demonstrate the ongoing adequacy of EIMT regimes by describing plant failures, anomalies and the means of rectification. Confirmation should be provided that cumulative data from EIMT continues to support the reliability claims made within security plans.

15. END OF ROUTINE OPERATIONS AND DECOMMISSIONING

15.1 Dutyholders may be able to justify reductions in EIMT for the various phases of facility decommissioning where site categorisation for theft and sabotage may decrease and a less onerous outcome be required of the PPS. However, any such reduction should be supported by amended security plans that demonstrate the revised arrangements are adequate.

Inspectors Should Consider

- Does the dutyholder have adequate arrangements for maintaining installed security equipment prior to it being put into operational service?
- Is the EIMT programme adequate to maintain the current (and/or future) PPS posture, outcome and the associated nuclear security functions identified in security plans?
- Do dutyholders have a process for capturing project assumptions related to EIMT generated by the on-going design and security analyses, along with an auditable record of where these assumptions are recorded in operational documents?
- Whether it is appropriate for the EIMT programme for the PPS to be aligned with any other EIMT programme on site?
- Does the EIMT strategy ensure that adequate compensatory measures have been identified and implemented to allow security important equipment to be released for EIMT?
- Does the proposed EIMT strategy support security plan reliability claims?
- Is adequate development work undertaken on novel systems or components between concept design and manufacturing? Such work may have significant impact on the EIMT tasks defined within the evolving maintenance schedules.
- Are all relevant stakeholders involved in developing an appropriate EIMT programme for the PPS?
- Has the dutyholder adequately incorporated human factors assessments of EIMT tasks during testing and commissioning? Looking in particular, for error

traps, and common cause failure mechanisms created by the procedures or by operators' actions.

- Whether the EIMT specified, and standards selected, for the various SSCs, are to a level of quality commensurate with their security classification?
- Are the dutyholder's arrangements for developing a catalogue of all facility EIMT adequate and items important to nuclear security are placed on the Plant Maintenance Schedule?
- Where in situ testing is not possible, are alternative arrangements made by the dutyholder adequate? Such alternative arrangements may be necessary for issues such as the removal and rig-testing of a device.
- Are security plan assumptions regarding component reliability, which can influence "mean time between failures" and therefore tests and performance, along with unavailability for EIMT, adequately reflected in implementation documentation such as Maintenance Schedules and Instructions?
- Do EIMT instructions provide for full and accurate reporting? This should include the recording and reporting of any defects and of any properties or parameters which may need to be monitored to confirm continuing safe operation. Clear criteria for successful completion of the work should be stated and the procedures should provide for the reporting and rectification of non-conformances.
- Are arrangements in place to identify trends in failures or gradual degradation of security equipment over time?
- Are both security plan and plant changes adequately assessed by appropriate SQEP staff to identify commensurate effects on the existing EIMT arrangements and the need for any additional EIMT? Such changes may result in the need to modify the Maintenance Schedules and Maintenance Instructions.
- Does the dutyholder have adequate EIMT arrangements for equipment provided to support the site's and facility's security response?
- Are there adequate provisions for the secure, quarantined storage of overhauled security equipment prior to it being re-installed on the facility?
- Are dutyholders are adopting the latest good practices for EIMT?
- Do dutyholders have a formal process for EIMT staff to identify shortfalls, inconsistencies or discrepancies in EIMT procedures, along with evidence that staff are encouraged to use the process; that the process provides a mechanism for dealing with the observations raised and learning from experience?
- Are the dutyholder's maintenance arrangements based on generic approaches? Such approaches could include: reliability-centred maintenance, condition monitoring, planned maintenance, preventative maintenance, risk-based maintenance and run-to-failure (corrective) maintenance.

16. 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. 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://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

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

8. **Nuclear Industries Malicious Capabilities Planning Assumptions.**

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

17. GLOSSARY AND ABBREVIATIONS

CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
EIMT	Examination, Inspection, Maintenance and Testing
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
PPS	Physical Protection System
R&D	Research and Development
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SSC	Security Structure, System and Component
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide