ONR GUIDE			
RELIABILITY, RESILIENCE AND SUSTAINABILITY			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-5.0 Revision 0		
Date Issued:	January 2018	**Review Date:**	January 2021
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	TRIM Folder 4.4.2.20789. (2017/456595)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 01/18

1 INTRODUCTION

1.1 The Nuclear Industries Security Regulations (NISR) 2003 contains requirements for responsible persons to make certain arrangements including standards and procedures to ensure the security of the nuclear premises, Nuclear Material (NM) stored on the premises, Sensitive Nuclear Information (SNI) and standards and procedures for the transportation of Category I - III NM.

1.2 Regulation 4 of NISR requires there to be an approved security plan for each nuclear premises which details those arrangements for the protection of NM/ORM and SNI, including contingency plans. Regulation 7 places the requirement for the dutyholder to maintain arrangements in accordance with the approved plan. Similarly, transporters of Category I-III quantities of NM are required to detail their security arrangements in an approved Transport Security Statement in accordance with Regulation 16 and Regulation 17 requires them to maintain those arrangements. For the purposes of this guide, the term security plan will be used to refer to both approved documents.

1.3 The Office for Nuclear Regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 5.1) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

1.4 To assist inspectors, ONR produces a suite of guides to assist them in making regulatory judgements and decisions in relation to the adequacy of compliance. This inspection guide is one of the suites of documents provided by ONR for this purpose.

2 PURPOSE AND SCOPE

2.1 Security plans are structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guidance is to facilitate a consistent and effective approach to FSyP 5 - Reliability, Resilience and Sustainability. This fundamental principle is supported by three Technical Assessment Guides (TAGs): Reliability and Resilience (Reference 5.2); Examination, Inspection, Maintenance and Testing (Reference 5.3); and Sustainability (Reference 5.4).

2.2 The judgements made by the inspector will primarily relate to the efficacy of the implementation of arrangements described in evidence that supports the security plan to ensure that associated arguments are fully substantiated. However, ONR takes a sampling approach to regulation and it is possible that elements of evidence within the plan were not subject to assessment as part of the approval process. Therefore, when reviewing or inspecting evidence as part of the intervention, the judgement may relate to the efficacy of the evidence itself in relation to supporting any associated arguments. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 This guidance is not intended to be mandatory, but provides a framework for inspectors on which to base their judgement and discretion during such inspections.

2.4 This guidance does not indicate when or to what extent these compliance inspections should be made. These matters are covered in the integrated intervention strategy and individual inspectors' inspection plans.

2.5 This guide lays the foundation for all inspection activities carried out by CNS inspectors. The same basic phases should be applicable to an inspector in any of the ONR Divisions. The phases which will help inspectors plan their inspection programmes are: planning, preparation, delivery, write up, and follow up. For more detailed information on these phases see ONR Guide GD-064 (Reference 5.5).

2.6 The guidance contained in this document is consistent with International Atomic Energy Agency (IAEA) Safety Standard No GS-R-3 (The Management System for Facilities and Activities) which equally applies to safety and security and is applicable to the activities of all dutyholders (Reference 5.6).

2.7 The IAEA Nuclear Security Fundamentals NSS 20 dated February 2013 (Reference 5.7), Article 3.12 requires Member States to ensure that dutyholders establish and implement an effective integrated management system and demonstrate leadership in nuclear security matters. SyAPs transposes this requirement in the UK and this guidance considers the relevant aspects of Reliability, Resilience and Sustainability.

3 OVERVIEW OF FUNDAMENTAL SECURITY PRINCIPLE 5: RELIABILITY, RESILIENCE AND SUSTAINABILITY

3.1 FSyP 5 requires dutyholders to design and support their nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle.

3.2 SyDP 5.1 describes how security structures, systems and components should be appropriately qualified, with design incorporating reliability and resilience through ‘failsecure’, redundancy, diversity and segregation. There should also be sufficient resources available and contingency arrangements developed to ensure continuity of security provision.

3.3 SyDP 5.2 outlines that security structures, systems and components should receive regular and systematic Examination, Inspection, Maintenance and Testing (EIMT).

3.4 SyDP 5.3 details that 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.

4 GUIDANCE ON THE EXPECTATIONS FOR THE INSPECTION OF FSYP 5

Phases – General

4.1 ONR CNS has developed a regulatory strategy for dutyholders. This includes undertaking a programme of Reliability, Resilience and Sustainability interventions to influence behavioural changes across the industry. For all of the major sites and facilities, an annual Integrated Intervention Strategy (IIS) exists which describes how the strategy is realised through a series of planned inspections. For more detail on IIS plans, see ONR Guide GD-059 (Reference 5.8).

Taking into Account Other FSyPs

4.2 Inspectors should take into account other FSyPs when carrying out Reliability, Resilience and Sustainability inspections, in particular: FSyP 3 (Competence Management). For example, inspectors should determine whether dutyholder’s staff are suitably qualified and experienced to carry out their assigned EIMT roles and responsibilities?

Implementation

4.3 Information on implementing the planning, preparation, delivery, write-up and follow up phases are contained in ONR Guide GD-064 (Reference 5.5).

Specific Advice for Reliability, Resilience and Sustainability Inspections

4.4 Specific considerations related to the arrangements for each of the FSyP elements are covered in the Annexes as follows:

- Annex A - SyDP 5.1 (Reliability and Resilience).
- Annex B – SyDP 5.2 (Examination, Inspection, Maintenance and Testing).
- Annex C – SyDP 5.3 (Sustainability).

5 FURTHER READING

5.1 Security Assessment Principles for the Civil Nuclear Industry.

5.2 CNS-TAST-GD-5.1 - Reliability and Resilience.

5.3 CNS-TAST-GD-5.2 - Examination, Inspection, Maintenance and Testing.

5.4 CNS-TAST-GD-5.3 - Sustainability.

5.5 ONR GUIDE GD-064 – General Inspection Guide.

5.6 IAEA Safety Standard No GS-R-3 (The Management System for Facilities and Activities).

5.7 IAEA Nuclear Security Fundamentals NSS 20.

5.8 ONR Guide GD-059 - Guidance for Intervention Planning and Reporting.

6 ANNEX A - RELIABILITY AND RESILIENCE

Regulatory Expectation

The regulatory expectation is that dutyholders demonstrate in their security plan how they ensure that the design and operation of the security system delivers appropriate levels of redundancy, diversity and segregation. Dutyholders should provide sufficient resources (including personnel) to inform the design, to maintain and to restore nuclear security structures, systems and components (SSCs), thus building resilience to enable an appropriate and effective incident response, and a recovery programme that reflects a proportionate response to the risk of any loss of service. Essential services critical to the correct functioning of the security system should be given the same priority as the system itself, and as such are required to have appropriate levels of reliability and resilience.

Inspectors should consider the dutyholder's ability to demonstrate compliance with arrangements made in their security plans through the exhibition of behaviours and knowledge, and the provision of evidence which may consider:

- Has reliability, resilience and sustainability been considered throughout the design stage for any new facility or security system? Has it been incorporated within the relevant operational requirements documentation?
- Are the requirements for security systems regularly reassessed?
- Are there sufficient Suitably Qualified and Experienced (SQEP) personnel and other resources to manage, operate, maintain and repair the security system?
- Are the competencies required to sustain a nuclear security workforce maintained through recruitment, retention and training?
- Does the design and operation of the security system display appropriate levels of redundancy, diversity and segregation?
- Do essential services (such as power) necessary for the correct functioning of the security system have the appropriate levels of security, reliability and resilience?
- Have the potential dependencies and/or vulnerabilities of the security system been identified and mitigated?
- Are the claims and assumptions contained in design and procurement documents?
- Do security systems 'fail secure' and if they do not, are security requirements appropriately balanced against safety requirements and adequate compensatory security measures available?
- How do the relevant personnel learn from experience of maintaining the security system and is this learning captured and distributed?
- Is the dutyholders' experience of security system failure and breakdown in line with reliability claims, trends and recovery and substitution arrangements?
- Is there a process of continuous improvement in place relative to the security system's reliability, resilience and sustainability?
- How are quality performance and assurance mechanisms applied to security systems?
- Is there any evidence that the response to the failure or loss of part, of or all of, a security SSC is regularly exercised or rehearsed?

The following documents are representative of evidence that may be referenced in the security plan and they could be sought for review prior to the inspection:

- Relevant security plans.
- Relevant policies and procedures.
- Training records.

7 ANNEX B - EXAMINATION, INSPECTION, MAINTENANCE AND TESTING

Regulatory Expectation

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. There should be traceability of EIMT requirements from the security plans through the plant maintenance schedule to maintenance instructions.

Inspectors should consider the dutyholders ability to demonstrate compliance with arrangements made in their security plans through the exhibition of behaviours and knowledge, and the provision of evidence which may consider:

- Has the dutyholder defined adequate arrangements for maintaining installed, or permissioning new security equipment prior to it being put into operational service?
- Is the EIMT programme adequate in order to maintain the current (and/or future) PPS posture, outcome and associated nuclear security functions identified in security plans?
- Do the 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?
- Are the EIMT arrangements consistent with those identified in the security specification?
- Does the EIMT strategy ensure that adequate compensatory measures or substitution arrangements 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?
- Has adequate development work been undertaken on novel systems or components between concept design and manufacturing? Does EIMT adopt a flexible approach during this phase incorporating learning from experience and a formal review of findings prior to manufacture?
- Have stakeholders developed an appropriate EIMT programme for the PPS?
- Where multiple dutyholders exist within one geographical site, are there appropriate, documented arrangements to define who is responsible for the EIMT of each SSC for security?
- Where there are SSCs that relate to both nuclear safety and nuclear security, are there appropriate, documented arrangements in place to define who is responsible for EMIT of each SSC? Are there mechanisms to ensure certain SSCs not overlooked?
- Has the dutyholder adequately incorporated human factors assessments of EIMT tasks during testing and commissioning? Look in particular for error traps and common cause failure mechanisms created by the procedures or by operator actions.
- Are the SSCs appropriately classified and prioritised for EIMT? Is the EIMT frequency suitably informed by the classification of the SSC?
- Is EIMT carried out within the specified intervals?
- Is EIMT carried out by SQEPs using appropriate tools and procedures and calibrated using verified sources/check gauges?
- Are security SSCs brought into service by an appropriate and suitably qualified, experienced and designated person?

- Are changes to EIMT periodicity or arrangements subject to suitable change control?
- Are the dutyholder's arrangements for developing a catalogue of all facility EIMT adequate, and have items important to nuclear security placed on the Plant Maintenance Schedule and subject to periodic review? Is EIMT carried out in all appropriate facilities?
- Are maintenance backlogs kept under review and minimised?
- Are defect tags used, kept under review and sentenced appropriately?
- Where in situ testing is not possible, are the alternative arrangements made by the dutyholder adequate?
- 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?
- Are EIMT instructions provided for full and accurate reporting and are written instructions followed and traceable? Does this 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? Are clear criteria for successful completion of the work stated and are there laid down procedures 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 security plans and plant changes adequately assessed by appropriate SQEP staff to identify unrealised effects on the existing EIMT arrangements and/or the need for any additional EIMT? Have maintenance schedules and maintenance instructions been modified accordingly?
- Does the dutyholder have adequate EIMT arrangements for equipment provided to support the site's and facility's security response?
- Have adequate provisions for the secure, quarantined storage of overhauled security equipment been provided prior to it being re-installed on the facility?
- Does the dutyholder adopt the latest relevant good practices for EIMT?
- Do dutyholders have a formal process which enables EIMT staff to identify shortfalls, inconsistencies or discrepancies in EIMT procedures:
  - Is there evidence that staff are encouraged to use the process?
  - Does the process provide a mechanism for dealing with the observations raised and learning from experience?
- Where EIMT is outsourced to a contractor, does the dutyholder effectively manage the contract and maintain an intelligent customer capability? Are any service level contracts/agreements regularly reviewed to ensure they are fit for purpose?
- Are the dutyholder's maintenance arrangements based on generic approaches? Is the approach appropriate to the importance of the SSC in delivering the outcome? How has the dutyholder confirmed this is kept under review in light of defects, failures and performance degradation over time? Such approaches could include:
  - Reliability-centred maintenance.
  - Condition monitoring.
  - Planned maintenance.
  - Preventative maintenance.
  - Risk based maintenance.
  - Run-to-failure (corrective) maintenance.

The following documents are representative of evidence that may be referenced in the security plan and they could be sought for review prior to the inspection:

- Relevant Security plans.

- Relevant policies and procedures.
- Training records.
- Plant maintenance schedules.
- Maintenance instructions.
- Quality plans.
- Maintenance records.
- Configurations of operational security systems.
- Temporary security plans.
- Vulnerability analysis.
- Risk assessments.
- Inspection reports.
- Human factors assessments

8 ANNEX C - SUSTAINABILITY

Regulatory Expectation

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.

Inspectors should consider the dutyholders ability to demonstrate compliance with arrangements made in their security plans through the exhibition of behaviours and knowledge, and the provision of evidence which may consider:

Managing and Planning for Sustainable Operations

- Do SQEP senior managers set priorities and determine the long term costs associated with the design, operation and maintenance of nuclear security systems and measures?
- Is there a programme which reviews security arrangements to ensure suitable replacement and refreshment?
- Are security arrangements reviewed after periods of increase security activity, such as increased threat levels, to ensure learning is taken into account and sustainability plans updated when appropriate?
- Are relevant management decisions documented as part of a formal approval process?
- 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.
  - Repetition and improvement of the process.

Applying Configuration Management

- Does the dutyholder apply configuration management to document the physical, procedural and training elements of its critical nuclear security systems?
- How does the dutyholder ensure configuration management information is:
  - Accurate?
  - Available in a timely manner?
  - Appropriately protected?
- How does the dutyholder ensure that the security implications of changes in nuclear security systems are subject to configuration management and are reviewed prior to implementation and documented appropriately?
- How does the dutyholder ensure that the security implications of changes in other systems that have an impact on nuclear security are reviewed prior to implementation, and are documented appropriately?
- How does the dutyholder identify critical nuclear security systems and determine appropriate protection?

Conducting Compliance and Performance Evaluations

- Does the dutyholder implement formalised and documented compliance and performance evaluations?
- Are vulnerabilities mitigated to agreed timescales (e.g. in line with the security plan improvement schedule)? Is an evaluation undertaken of the progress in addressing the identified shortcomings?
- Does the dutyholder validate functional requirements and performance of security systems? Does the dutyholder use the security plan to provide a basis for the design, frequency and performance criteria for the testing programme? Do these evaluations verify that the criteria for reliability, operability, readiness and performance are met?
- Has the dutyholder ensured 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, reports 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 relevant results?
- Does the dutyholder ensure that tests are conducted rotationally to verify that all human factor contributions to security sustainability are assessed?

The following documents are representative of evidence that may be referenced in the security plan and could be sought for review prior to the inspection:

- Relevant security plans.
- Relevant policies and procedures
- Security asset management plans
- Documented management decisions.
- Risk assessments.
- Threat assessments
- Relevant procedures.
- Security performance assessments.
- Security personnel strategies