ONR GUIDE			
TESTING AND EXERCISING THE SECURITY RESPONSE			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-10.2 Issue 2.1		
Date Issued:	October 2020	**Review Date:**	October 2024
Approved by:	Matt Sims	Professional Lead	
Record Reference:	CM9 Folder 4.4.2.23373. (2021/61627)		
Revision commentary:	Reference 8 updated.		

TABLE OF CONTENTS

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 (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 arrangements to test and exercise the security contingency response. 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 emergency preparedness and response to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND OTHER 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 Principles K of the CPPNM refers to the production of contingency plans and states that contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned. The importance of issues relating to testing and exercising, particularly in preparation for and response to a Nuclear Security Event (NSE) is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 11: Planning for, Preparedness for, and Response to, a NSE, paragraph 3.11 - A nuclear security regime ensures that relevant competent authorities and authorised persons are prepared to respond, and respond appropriately, at local, national, and international levels to NSEs by:

  b) Periodically exercising, testing, and evaluating the plans for effectiveness by relevant competent authorities and authorised persons with the aim of ensuring timely implementation of comprehensive measures to:

    i) mitigate and minimise harmful consequences to persons, property, society, and the environment from NSEs;

    ii) locate, recover, and secure nuclear material and other radioactive material that is out of regulatory control; and,

    iii) feedback into the preparedness process, including into the response plans, the results of exercises and tests of the plans, and of experience.

- Essential Element 12: Sustaining a Nuclear Security Regime, paragraph 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:

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

  f) having in place processes for using best practises and lessons learned from experience; and,

  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, always.

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 2). This document states that the coordination between the guards and response forces during a NSE should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the guards, response forces and other response teams for implementation of the plans.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 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 10.2 – Testing and Exercising the Security Response, in support of FSyP 10 – Emergency Preparedness and Response. 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 Effective response arrangements to a NSE are an integral part of the overall strategy for ensuring nuclear or other radioactive material and any associated vital areas are properly secured. Maintenance of an exercise programme, stringent self-evaluation via Security Contingency Exercise (SCX) reports and decisively acting on lessons identified are key indicators of a dutyholder's understanding of the importance of an effective security response.

6.2 Exercising allows for personnel with emergency and security response responsibilities to be trained in the Security Contingency Plan (SCP). It also provides an opportunity to rehearse the arrangements described in the SCP and test their effectiveness. Therefore, security response drills should be undertaken regularly if staff and contractors are to be familiar with procedures, the actions to be taken and their responsibilities in the event of a real or suspected NSE.

6.3 Dutyholders are also expected to deliver a **Regulator Evaluated Demonstration Exercise (REDE)**. However, these are a demonstration of capability and should not be used for training or rehearsal of plans. Further information on ONR-observed exercises can be found in technical inspection guide CNS-INSP-GD-001 (Reference 8).

6.4 This TAG informs regulatory assessment of the dutyholder's Emergency Preparedness and Response arrangements from a security perspective, arrangements for testing and exercising of the SCP.

Regulatory Expectations

6.5 The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how they maintain an effective programme to test and exercise the SCP.

FSyP 10 - Emergency Preparedness and Response	Testing and Exercising the Security Response	SyDP 10.2
Dutyholders should implement a regime of exercising to train personnel and test the efficacy of the nuclear security contingency plans.		

7. GUIDANCE ON ARRANGEMENTS FOR TRAINING AND DELIVERY OF A REDE

Training Programme

7.1 The dutyholder should deliver a training programme that:

a) Ensures members of Site Emergency Organisation (SEO) are trained and remain competent to be suitably qualified and experienced persons (SQEP) for their role and responsibilities as required under the SCP.

b) Demonstrates SEO integration and interoperability in order to deliver the required PPS Response and Required Effect in an effective and timely manner.

c) Conducts an appropriate combination of 'live' and 'table-top' Security Contingency Exercises (SCXs) at regular intervals throughout the year, that is comparable to safety exercise activities

d) Includes, wherever possible, external stakeholders (e.g. first responders). If they cannot attend, the dutyholder should ensure any equivalent notional external stakeholder 'play' during a SCX accurately reflects the stakeholder's tactics, techniques and procedures.

e) Implements an assurance regime for SCXs and associated training, in order that:

i) Activities are recorded at individual and collective level

ii) Performance is assessed and reviewed objectively and documented, with good practice and learning points incorporated into the SCP and used to inform future training needs and plans.

f) SCXs should reflect the same planning principles as described at Para's 7.5-7.8 and must provide the same arrangements as stated at Para 7.9.

DELIVERY OF A REDE

7.2 ONR promotes an enabling approach to outcome focussed regulation, which acknowledges the benefits of reducing the regulatory burden to the dutyholder wherever possible. Accordingly, we acknowledge that an informed, risk-based approach to dutyholder's demonstrations of their arrangements should be proportionate and (potentially) achievable.

7.3 As part of the non-prescriptive SyAPs approach, there is no automatic expectation that sites should demonstrate annually, although delivering a 'regular' demonstration (as specified in NISR) is unlikely to be less frequent than once per year unless in exceptional circumstances. Regulatory judgements are likely to be delivered on a site-by-site basis and based on the relevant ONR site inspection team's analysis. The form of demonstration, depending on regulatory judgement, can be either a full practical REDE or a combination of a tabletop/command-post exercise.

7.4 Expectations are to be based on the NM/ORM holdings and VAs (if any), risk and threat profile of the site. Other key factors to consider will include; outstanding regulatory issues as a result of the dutyholder previous demonstration and adequacy of extant arrangements of the dutyholder's training, testing and exercising regime for the SEO.

REDE Planning Process

7.5 The dutyholder should deliver a planning process that:

a) Secures agreement from the ONR inspector for an ONR observed 'live play' or 'table-top' REDE in a timely manner to allow for annual planning processes.

b) Ensures that the CNC (where deployed) give prior agreement to the date for a REDE.

c) Conducts an initial planning meeting (excluding exercise participants), no less than 6 months before the date of the exercise. The meeting should be attended by the ONR security inspector and/or ONR emergency preparedness and response security inspector. The draft exercise objectives and success criteria should be forwarded to the ONR security inspector prior to the meeting. Where appropriate a representative from the CNC (where applicable) and any other relevant stakeholders (internal and external) should also attend these meetings. Subsequent meetings to develop the scenario should be held as required with the ONR inspector attending where needed.

d) Ensures all elements of the SEO are exercised. In addition, an agreed and meaningful proportion of the work force is to take part in the demonstration.

e) Produces an exercise instruction that is forwarded to reach ONR no later than four weeks prior to the date of the exercise.

f) Undertakes a REDE review meeting (to be attended by all relevant stakeholders) no later than six months after the REDE has taken place.

Objectives, Success Criteria and Scenarios

7.6 The dutyholder should:

a) Maintain a record/matrix to ensure all aspects of the SCP are exercised against relevant threats within a reasonable period.

b) Ensure the objectives, success criteria and scenario for the SCX are agreed with ONR in advance prior to the initial planning meeting.

c) The objectives and success criteria should be decided first and then applied to a scenario that allows the SCP to be demonstrated in a proportionate manner. They should:

   i) Be challenging and fully expose security contingency planning and response to a NSE.

   ii) Reflect multiple aspects of the SCP, elements of the emergency plan and/or handbook.

   iii) Challenge the Command, Control and Communication (C3) of the SEO at OPERATIONAL and TACTICAL levels, and the integration of external stakeholders.

   iv) Require exercise participation at all levels, from OPERATIONAL first responders to TACTICAL actions of personnel in command roles.

   v) Consider previous REDEs both in terms of the malicious scenario chosen and any learning points arising. Unless a requirement of ONR, the dutyholder should ensure that differing DBT actors are used than that on previous demonstrations.

   vi) Be agreed by all stakeholders.

   vii) Driven by the security outcome required of the Physical Protection System (PPS) and associated response as defined in Annex C and D of SyAPs.

d) ONR have delivered a number of ‘REDE planning workshops’ to dutyholders, with the aim of assisting planners in understanding and meeting regulatory expectations in delivering a REDE. This has included a range of generic objectives that could be applied across the SEO response. These objectives could also be useful in assisting planners in identifying what success criteria could be needed to deliver objectives and thus inform the construct of the scenario. These are:

   - To establish and maintain a comprehensive understanding of the situation, to cater for the worst credible developments, formulate measures and plans to achieve recovery and prevent deterioration of the situation.

   - Mobilise, deploy and direct appropriate resources in the most effective and timely manner.

   - Demonstrate site's ability to mitigate the security, safety and environmental threats posed.

- Ensure adequate arrangements are in place for the arrival of external responders, including an effective process for their reception, staging and onward integration.

- Demonstrate adequate consideration and arrangements for preservation of a crime scene and concurrent post-incident recovery.

- Make adequate arrangements to notify all external agencies and for responding to public and media enquiries

- To ensure a comprehensive record of events and decision rationale is taken for evidence preservation, for use in informing subsequent investigations.

7.7 The dutyholder could consider a flexible approach towards achieving objectives and success criteria within the exercise through incorporating a series of scenarios in order to demonstrate a range of capabilities in responding to an NSE. Use of a phased approach may offer the following opportunities:

- **Phase 1** - **Immediate Response**. Phase 1 could allow the dutyholder, in conjunction with the CNC and/or other on or off-site responders, to demonstrate operational capability against a credible threat. Where applicable it will involve the CNC (where deployed), the Civilian Guard Force (CGF), host police force first responders and all C3 elements of the Site Emergency Organisation (SEO).

- **Phase 2 – Event Management**. Phase 2 could allow the dutyholder to demonstrate effective management of the event, integrated with all relevant supporting agencies and responders. The same scenario as Phase 1 or a completely different one can be used.

- **Phase 3 – Consequence Management**. Phase 3 could allow the dutyholder to demonstrate an understanding of the post-incident recovery and their facilitation of crime scene management in a response to a NSE. Phase 3 would typically be exercised via a table-top exercise. As with phase 2, it may utilise the same scenario as earlier phases or have a completely different one, depending on the exercise objectives and success criteria.

Malicious Actor(s)

7.8 The dutyholder should:

a) Include malicious capabilities drawn from the extant United Kingdom Design Basis Threat (UKDBT) document. Specifically, they should identify a malicious actor(s) with target objectives that accords with the category of the site, which can be used to realistically test arrangements across all phases of the site's response to an NSE. The arrangements should demonstrate that the Physical Protection System (PPS) Response and Required Effect can consistently and effectively be delivered in order to achieve the required security outcome.

b) Ensure REDEs are conducted using 'live-play' malicious actors, based on relevant threats and capabilities given in the UKDBT, and that the scenario(s) properly reflects the consequence of compromise (theft and sabotage) of the NM/ORM/VAs and facilities on the site. On sites required to meet PPS Outcome 4, a malicious presence on site may not be required and subject to approval from ONR the malicious actor could be simulated.

c) Consider utilising the Potential Adversary Forces (PADFOR) Handbook to inform exercise planners and controllers on possible TACTICAL and OPERATIONAL target objectives of the adversaries who are conducting malicious acts.

Maintain the Security of the Site

7.9 The dutyholder should ensure the security of the site is maintained whilst the REDE and associated training is being conducted. Measures that could be considered include:

a) Compensating for the abstraction of personnel who are attending training by deploying additional SQEP staff to undertake the roles of those engaged in training.

b) Develop temporary security plans, where appropriate, for approval by ONR before any activity takes place. For example, this could be for buildings left insecure post-evacuation.

Inspectors should consider:

- Does the security plan define an effective REDE delivery process and training programme for the Site Emergency Organisation (SEO)?
- Are all relevant stakeholders involved in the exercise and training programme planning process?
- Is there a structured and informed planning process to facilitate a REDE?
- Is there an audit in place that records individual and collective training in delivering roles, responsibilities and required effects of the SCP?
- Is there an audit of performance assessment of the SEO undertaking SCXs?
- Are a range of SCX scenarios, objectives and success criteria developed that are specific to the site characteristics?
- Does the security plan ensure that the dutyholders' REDE and SCXs demonstrate their arrangements across the immediate response, event management and consequence management phases of a response to a NSE?
- Does the security plan require realistic SCX scenarios that reflect relevant UKDBT capabilities and the required PPS Response and Required Effect for the site?

- Does the security plan require that a formal review of SCXs is undertaken and that good practice and learning points is disseminated to relevant stakeholders?

- Does the security plan ensure that the PPS of the site and key facilities is maintained throughout a SCX /REDE?

8. 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/publications/security-policy-framework/hmg-security-policy-framework

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

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

8. **ONR Technical Inspection Guide CNS-INSP-GD-10.0 Revision 2**. Emergency Preparedness and Response. https://www.onr.org.uk/operational/tech_insp_guides/cns-insp-gd-10.0.pdf

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

9. GLOSSARY AND ABBREVIATIONS

C3	Command, Control and Communications
CNC	Civil Nuclear Constabulary
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
NSE	Nuclear Security Event
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
REDE	Regulator Evaluated Demonstration Exercise
SCX	Security Contingency Exercise
SCP	Security Contingency Plan
SEO	Site Emergency Organisation
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
UKDBT	United Kingdom Design Basis Threat