1

ONR GUIDE			
CT MEASURES, EMERGENCY PREPAREDNESS AND RESPONSE PLANNING			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-10.1 Revision 2		
Date Issued:	October 2020	**Review Date:**	October 2024
Approved by:	Matt Sims	Professional Lead	
Record Reference:	CM9 Folder 4.4.2.23373. (2020/273831)		
Revision commentary:	Fit For Purpose Review of Rev.1 resulted in amendments to paragraphs: 6.2 correct nomenclature, 9.2 wording change to reflect IAEA guidance, the term 'suspected to cause' introduced for suspect devices, term 'host police forces' replaces 'home office' in the main text, 11.2 reference to CS&IA contingencies, 15.2 new term 'minimum' safety distances, 16.1 reference to 'reception briefs' for emergency responders, 16.2 reference to Joint Services Interoperability Programme (JESIP) and Action Counters Terrorism (ACT) initiatives. Consequence Management – OPEX update.		

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 considered 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 Counter Terrorism (CT) measures and Emergency Preparedness & Response (EP&R) planning arrangements. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers 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 Principle 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.

4.3 The importance of issues relating to command and control during Nuclear Security Events (NSEs) is also recognised in the Nuclear Security Fundamentals, specifically Essential Element 11: Planning for, preparedness for, and response to, a nuclear security event, paragraph 3.11 which states that 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:

a) Developing arrangements and response plans for ensuring:

i) rapid and effective mobilisation of resources in response to a NSE; and,

ii) effective coordination and cooperation during response to a NSE among all those carrying out response functions (including intelligence, law enforcement, crime scene investigation, and nuclear forensics) and between the security and safety aspects of the response.

4.4 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). In relation to contingency plans, this document states that:

- Dutyholders should prepare contingency plans to effectively counter the threat assessment or design basis threat taking actions of the response forces into consideration.
- The dutyholder's contingency plan should be approved by the State's competent authority as a part of the security plan.
- Arrangements should be made to ensure that during emergency conditions and exercises, the effectiveness of the Physical Protection System (PPS) is maintained.
- The operator should initiate its contingency plan after detection and assessment of any malicious act.

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 10.1 – CT Measures, Emergency Preparedness and Response Planning, 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 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 The national approach to providing CT protection, developed and circulated by the Cabinet Office National Security Secretariat, has been adapted by ONR to meet the requirements of the civil nuclear industry. The approach seeks to protect against malicious incidents directed at Nuclear Material or Other Radioactive Material (NM/ORM) and any associated Vital Areas (VAs).

6.2 Changes in the threat level will be issued by the Cabinet Office and industry is informed through the Civil Nuclear Constabulary (CNC) Command and Control Centre (CCC) at Culham. As part of emergency preparedness planning dutyholders should develop appropriate incremental and escalatory protective and physical security measures that can be quickly implemented in response to increases in threat. These measures should be identified within a dutyholder's security plan.

6.3 A dutyholder's Security Contingency Plan (SCP) provides a framework for the Site Emergency Organisation (SEO) and supports an effective response to a NSE. The key aspect in relation to a SCP are the 'steps to be taken' by the responsible person in directing the response to malicious events. Additionally, the SCP should reflect the regular practice of the activities required in connection with those steps and the standards, procedures and arrangements contained therein. This expectation seeks to ensure those responding to certain events, including the potential nuclear safety implications of the event, have, and are trained in, the use of, adequate guidance and a framework for decision making. This is so the SEO functions effectively under potentially hostile and adverse conditions throughout the three phases (as described at paragraph 9.2 below) of a malicious event.

6.4 Wherever possible, the considerations in this TAG should be used by inspectors to assess the adequacy of EP&R arrangements for approved carriers. Additional factors will have to be considered in reaching a judgement when material is moved off-site.

Regulatory Expectation

6.4 The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how the site adopts incremental security measures in response to changes in threat and implements effective EP&R arrangements in response to an NSE.

FSyP 10 - Emergency Preparedness and Response	CT Measures, Emergency Preparedness and Response Planning	SyDP 10.1
Dutyholders should have in place incremental CT measures that can be implemented in response to changes in threat; and EP&R arrangements to deal with any nuclear security event arising on the site and their potential effects.		

7. COUNTER TERRORISM CONTINGENCY PLANNING

7.1 The Government Response Level System (GRLS) comprises three levels (see Annex A) each indicating a level of preparedness to counter the commensurate threat of terrorism. The response level for the nuclear industry is confirmed by the Civil Nuclear Security Intelligence Forum having considered direction from the Cabinet Office and/or specific intelligence relating to the nuclear industry.

7.2 For off-site office premises and non-nuclear buildings occupied on licensed sites and other non-licensed facilities, particularly those that have an obvious association with the civil nuclear industry, CT contingency measures are strongly recommended. In such cases the degree of protection that is put in place is a matter for company management.

7.3 The dutyholder's arrangements should provide robust notification procedures to ensure timely implementation and the mechanism to inform staff of changes in Threat and Response Levels.

7.4 Dutyholders should determine how CT protective security measures will interface with the company's business continuity planning. All relevant parts of the company should be involved in the production and review of SCP plans and be aware of them, for example communications groups for media handling in the event of an incident. CT protective security measures including contingency planning and exercising will need to be detailed or comprehensively referenced in security plans.

7.5 The dutyholder may exceptionally implement an increased response level in response to credible threat advice received directly from an authoritative and verified local or national source, or where the circumstances at the site warrant it. Should this situation arise, the company should immediately inform CNC (CCC) and ONR of the circumstances.

8. DEVELOPMENT OF THE SCP

8.1 Heads of Site/Site Directors should select Suitably Qualified and Experienced Person (SQEP) staff of appropriate seniority to take responsibility for the preparation, implementation and review of the SCP.

8.2 The SCP author will require support and input from a range of staff on a site. Liaison with key stakeholders[1] is also necessary throughout the drafting and review process. Such activity will ensure the SCP considers, and is complementary to, response plans operated and maintained by each relevant stakeholder. Evidence of such engagement also provides assurance that effective working relationships exist.

8.3 When developing SCPs at sites where there is a CNC presence, there should be full consultation between the CNC and site stakeholders (including those with responsibilities for Security, Safety and Emergency Preparedness). The consultation process should ensure SCPs are coherent, align with other plans, deliver maximum effect, clarify relationships between the 'supported and supporting' commanders and avoid misunderstanding. The CNC CCC and Operational Unit Commanders should maintain comprehensive instructions detailing the CNC's response to counter the threats detailed in the Design Basis Threat (DBT). These response plans are complementary to the SCP and

[1] Key stakeholders are considered to be the CNC (where deployed) and/or host police forces (Home Office Police/Police Scotland), Civilian Guard Force /in-house Guard Force and emergency first responders, i.e. Fire and Rescue and Ambulance Services. Military Explosive Ordnance Disposal (EOD) is also a key responder and should be considered where appropriate.

together they must enable interoperability, unified command and a coordinated and effective response to an NSE. There should be evidence that the dutyholder has sought theoretical and physical verification that the site's SCP, CNC response plans, and plans of all relevant emergency first responders, are mutually supportive and coherent to support delivery of the PPS Response and required effect.

8.4 Appropriately sanitised details of CNC actions in support of the SEO response could be included in the SCP. The inclusion of these details will assist SEO decision-makers understand the likely tactics, techniques and procedures that the CNC could deploy in response to a threat.

8.5 In order to enable interoperability, unified command and a coordinated effective response to an NSE, the SCP should be harmonised with other site emergency response plans and arrangements, such as the Emergency Plan, Emergency Handbook and LC11 arrangements. The SCP must clearly demonstrate how the decision-maker will interface with the site's wider safety, emergency and business continuity planning. There should also be evidence that the author of the SCP has worked with the authors of both the Emergency Plan and Handbook to ensure they are complementary. There should also be guidance to assist decision makers in assessing risk when priorities conflict, or if the plans recommend conflicting actions. For example, there should be clarity in how the SEO measures the benefit of moving personnel around site to repair vital plant, or extract them from a danger area, when the site is in lockdown.

8.6 On civil nuclear premises where there is more than one occupier or tenant, and at adjacent nuclear licensed sites, all parties should be aware of the requirement to maintain a SCP. Periodic joint reviews should be carried out to confirm all parties understand their individual and collective responsibilities. Adjacent or multi-occupant site SCPs must be complementary so that actions and responses are managed and coordinated effectively. This is particularly relevant where, for example, a service is provided by a single security force to co-located dutyholders. Evidence of such engagement will demonstrate that good working relationships exist.

9. STRUCTURE OF THE SECURITY CONTINGENCY PLAN

9.1 Dutyholders may decide on the content and layout of the SCP. However, its structure and internal referencing/indexing should:

- enable swift and accurate navigation to deliver a timely and effective response;
- be concise and simple to use (to aid rapid, informed decision making); and,
- guide the decision-maker on the considerations and actions needed to be taken by the SEO in response to/management of/recovery from, a malicious event.

9.2 The dutyholder should develop site-specific procedures, as part of the SCP, to be followed during an NSE, or the discovery of something that may cause (or suspected to cause) serious or imminent danger. Contingencies should be based on a series of activity lists, action checklists or other appropriate forms of decision support matrices to ensure the decision maker understands the actions that need to be considered by the SEO at each phase of the response. These phases should be as follows:

Phase	Objective	Effect

ONE	Immediate response	The OPERATIONAL response of site first-responders[2].
TWO	Event management	The integrated TACTICAL management of an event up to the threat being neutralised/risk reduced to the same level as at the start. This will likely involve external multi-agency emergency responders.
THREE	Consequence management	The integrated TACTICAL post-incident recovery and management of the security of any crime scene in conjunction with the CNC and/or host police forces. This may include STRATEGIC factors that impact upon the site.

9.3 Notwithstanding the style or structure, a dutyholder's SCP should include the following attributes:

- Full endorsement at Board level or equivalent.
- Development and maintenance in accordance with the site's quality assurance process.
- Provision of a rapid response to an NSE by specifying the processes and procedures for the assembly, organisation and deployment of essential personnel.
- Identification of clear lines of responsibility, legal obligations and associated delegated powers as necessary.
- Identification of the tasks which must be undertaken and achieved.
- Implementation by SQEP personnel at all levels.
- Full integration with all appropriate stakeholders such as CNC and host police forces.
- Alignment with all other response/emergency plans.

10. ENDORSEMENT AND OWNERSHIP OF THE SCP

10.1 The SCP should be overseen by the Board level member responsible for security. Accordingly, there should be a clear policy statement, endorsed by the Board/Head of Company, which recognises the need for a SCP and acknowledges the requirement for compliance with NISR 2003, which is the legislative basis for the protection of nuclear premises and the NM/ORM therein. The policy statement should also endorse the need for regular practice of the SCP. A site's compliance with the standards in the SPF (particularly those associated with implementation and use of the GRLS), will be viewed as good practice.

10.2 In order to confirm their enduring relevance and effectiveness, SCPs should be included in the annual security plan review process. This work can be evidenced through the inclusion of a review statement in the security plan. The review statement should include relevant changes to:

[2] This can include CNC, guard force or other site personnel.

- sector/UK threat and/or response levels
- site built and operational environs;
- changes within the site emergency plan/handbook, or key stakeholders' plans that are interlinked with the SCP.

10.3 Improvements and/or amendments to the SCP may be required following exercises, actual events, or compliance inspections and the dutyholder should have procedures to evidence change supported by strong operational experience processes.

10.4 The SCP should be maintained in accordance with the dutyholder's quality assurance policy and applied consistently to all relevant company sites and areas. The SCP should also contain details of the roles, responsibilities and positions of those individuals who have quality assured, managed and endorsed it. Equally, the assurance arrangements for the delivery of SQEP resource and response capability should be in accordance with the dutyholder's quality assurance policy and applied consistently to all relevant company sites and areas.

11. APPLICATION OF THE DBT, OTHER THREATS AND ROBUSTNESS OF THE SCP

11.1 Rather than tying the SEO to a rigid response process, contingency responses should deliver a framework within which informed, dynamic and rapid decision making can be undertaken to direct and support a progressive response to a threat. However, in all cases, the SCP should ensure the response can achieve the required security response outcome (as defined in Annex C and D of SyAPs) against relevant DBT threats. The SCP should be written in terms which are intelligible to non-security experts, guiding them through the anticipated actions and requirements of responders and outlining relevant secondary hazards.

11.2 The SCP must consider contingencies which clearly reflect relevant threat actors to the site, as laid out in the DBT document[3]. The contingencies in the SCP should take account of facilities or material which is vulnerable to the capabilities outlined in the DBT. Plans to deal with attempted and actual theft, and sabotage should be clearly articulated. The SCP should also reflect other relevant current generic terrorist or domestic extremist threats to mainland Great Britain. Such threats, even if deemed outside the DBT, should not be ruled out. There should also be alignment with relevant aspects of the dutyholders CS&IA contingency responses, where there is a need for first responders to undertake actions to support such responses.

11.3 To ensure the SEO actions are realistic and achievable across the three phases of response, contingency measures should be fully developed, both theoretically and practically. As a general rule, a SCP which has been validated through tabletop, computer based exercises, or any other form of drill and exercise, and involves all relevant agencies, is more likely to provide effective integrated responses to actual incidents. A SCP which has been developed purely theoretically cannot be expected to provide assurance. Accordingly, evidence of practical development, validation and resulting refinement with all relevant stakeholders is likely to receive regulatory endorsement.

[3] However unlikely a threat is assessed to be by a dutyholder, it should not be ruled out but should be subsequently planned for, unless there is sound justification for its exclusion.

11.4 The security plan should identify the arrangements for the protection of NM/ORM from theft and sabotage against the DBT. There is an expectation that within the constraints of the DBT an attacking force should be limited in its success. The dutyholder should also consider scenarios outside of the DBT or where the PPS has been ineffective in achieving the required security outcome, in order to mitigate the effects by putting plant or systems in a quiescent state if possible, or ensure that appropriate responders are informed in a timely manner. The list below is not exclusive or exhaustive and dutyholders should use judgement on applicability. Scenarios may include;

- Threats greater than the DBT which will impede or defeat the defending force
- The adversary cannot be adequately denied and so gains access to Vital Areas
- Nuclear material is stolen and taken off the Site
- Intruders are not immediately neutralised, and their containment becomes protracted

11.5 Where the CNC is established, the dutyholder should provide assurance that situations outside PPS outcomes are included within CNC Operating Procedures for the site. This will involve supporting planning arrangements with host police forces as part of the Coordinated Police Protocol.

11.6 The dutyholder should consider the implications of operating in a contaminated environment, other hazards or when external cordons are required to maintain the security of NM/ORM during an off-site nuclear emergency and the subsequent recovery phase.

12. ACCOUNTANCY OF PERSONNEL AT LOCKDOWN.

12.1 Whilst the primary role of the SCP is the protection of NM/ORM and any associated VAs, there is an expectation that dutyholders should be able to account for personnel during ‘lockdown’ within appropriate timescales in order to ensure that other legislative responsibilities are complied with. Additionally, emergency responders and other supporting agencies (e.g. Explosive Ordnance Disposal (EOD) teams) may require confirmation of personnel locations before they can fulfil their legal obligations and complete specific tasks that help protect NM/ORM, the public, plant and personnel. Arrangements should be in, or referenced within, the SCP.

13. CASUALTY MANAGEMENT

13.1 Arrangements for the safe and secure management of casualties arising from a nuclear security event should be in, or referenced in, the SCP. These should identify casualty treatment, triage systems, extraction and the procedures for the handover to the emergency services.

14. REPORTING ARRANGEMENTS AND MEDIA STRATEGY

14.1 The SCP should detail, in priority order, all mandatory reporting requirements which follow the identification of a NSE. It should be clear who is specifically responsible for reporting, what should be reported and how reports should be made. It could also usefully highlight those notifications by supporting agencies, (e.g. CNC) so the SEO can verify completion.

14.2 To swiftly and proactively manage the reactions of site personnel (warning and informing), the public and the media effectively, a media strategy should be included. The media

strategy should be coordinated and agreed with appropriate external stakeholders, principally the host police forces and the government department responsible for nuclear policy.

15. GUIDANCE AND SUPPORTING INFORMATION

15.1 Guidance and supporting information can be obtained from police Counter Terrorism Security Advisers, the Centre for the Protection of National Infrastructure, EOD, CNC (where deployed) and other supporting agencies.

15.2 The SCP should support rapid navigation for the user in order that timely informed decisions can be made. It should not contain an excessive amount of background information or training material that could hinder the operations of the SEO and their subsequent decision making. Key SEO roles and responsibilities should be outlined in the plan. Assurances that the SEO and responders are qualified and trained in the detail of the plan and their part in specific contingencies should be provided within the dutyholder's training audit. However, key reference material or aide-memoires which will ensure the correct steps are being taken, e.g. cordon distances, minimum safety distances, briefing/reporting templates and supporting mapping, should be included and internally referenced within the plan.

16. LIAISON AND RESPONSE WITH EXTERNAL AGENCIES INCLUDING POLICE CTSAs

16.1 When formulating SCPs, dutyholders should establish and maintain links with the host police force and other emergency first-responders. When these agencies arrive at a site, they will require effective security/technical briefs to highlight the nuclear safety and any other secondary hazard considerations, as well as detail of the ongoing situation. Such briefs will inform the actions of those responders and their framework should be included in the SCP. This will help ensure the site identifies and provides whatever is needed for the adequate reception, staging and onward integration of first responders. The plan should reflect that the dutyholder should be prepared to deliver reception briefs to emergency responders at any location on or off site.

16.2 Ultimately, the purpose is to ensure the response is timely, integrated and effective, and that command and control is unified. To underpin this, the plan should reflect relevant aspects of the UKs Joint Services Interoperability Programme (JESIP) and Action Counters Terrorism (ACT) initiatives. The plan (and its products) should feature terminology that can be understood by both the SEO and emergency responders.

16.3 CTSAs act as a conduit for host police force engagement with dutyholders, can contribute to response planning and share good practice on protective and physical security matters. The dutyholder should provide evidence of engagement with CTSAs in order to provide assurance that response planning has been conducted in concert with host police forces. Routine CTSA liaison is usually delivered via Operation SHIELDING meetings.

17. TRAINING STRATEGY TO DELIVER SQEP

17.1 The SCP should reference the training strategy to achieve SQEP SEO resource and appropriate site personnel responses to an NSE. The training regime should be maintained in accordance with the dutyholders' testing and exercising' policy and applied consistently to all relevant company sites and areas**.**

17.2 The inspectors' considerations for this part of the arrangements are set out in CNS-TAST-GD-10.2 Revision 2.

18. CONSEQUENCE MANAGEMENT

18.1 The site's primary security consideration post-incident should be the protection of NM/ORM and any associated VAs in accordance with the security plan. Accordingly, an effective post-incident reporting and review processes should be in place.

18.2 Following an incident, the protection of evidence to support legal requirements and provide intelligence for the wider police investigation will be essential. Accordingly, the SCP should provide guidance to the SEO on the measures that should be taken until police first responders (or CNC if deployed) take responsibility as the lead organisation for the scene. Arrangements for crime scene management should not impede the site's responsibilities for post-incident recovery that will involve the maintenance of security or the protection of the public, plant, personnel and the environment.

18.3 The site will be guided by the police as to their requirements to conduct the necessary investigations. The SCP should, however, set out guidance as to the likely considerations that the Command Team will need to address in order to support the Police whilst maintaining safe operations. This guidance should be based upon:

- The need to allow large numbers of police and other emergency responders, vehicles and equipment rapid access to the site (including facilitating associated briefings and health and safety measures)
- The requirement to continue to protect the site when guards and CNC (if deployed) and site personnel that have been involved in the NSE have been removed for investigation purposes
- The potential need for large scale searches and recovery operations to be conducted in order that the site can be declared safe
- The likely requirement for the police to obtain significant witness statements from staff immediately involved with the incident and subsequently, a potentially large proportion of the workforce who may have witnessed the event
- The likelihood that personnel will not be able to leave site unless under police arrangements.
- The need to appropriately address any welfare issues of personnel.
- An understanding that an investigation may take an extended and protracted period of time depending on the nature of the nuclear security event and the size and complexity of the site or facility

18.4 The above list is not exhaustive and simply gives an indication of what the inspector should be expecting to see. If these arrangements are held elsewhere then they should be referenced within the SCP.

Inspectors should consider:

- Does the SCP establish measures to deliver an appropriate, incremental and escalatory response to changes in the threat level aligned to the GRLS? Have all

relevant internal and external stakeholders been appropriately consulted during the preparation of the SCP?

- Is there evidence that contingencies have been theoretically and physically validated by all relevant stakeholders?
- Is there Board level endorsement and oversight of CT protection policy and implementation of the SCP?
- Do communication and information exchange arrangements and procedures provide an immediate notification of an increase in the response level (including staff awareness briefings)?
- Is the SCP an accessible, integral and well understood component of the security plan?
- Does the SCP address all relevant threats identified within the DBT and additional threats deemed relevant by the dutyholder?
- Does the SCP enable the PPS to be incrementally enhanced? For example, using additional patrolling, access control and search arrangements, minimising deliveries and visitors etc.
- Is the SCP appropriately integrated with other safety and security emergency response arrangements in order to deliver a holistic approach to emergency events?
- Are there enough SQEP staff available (including on call staff) within a dutyholder's emergency organisation to deliver an appropriate response in a timely and effective manner?
- Are adequate 'steps to be taken' included in the SCP, or appropriately signposted, and are they regularly practised? The assessment of testing and exercising emergency arrangements in response to a nuclear security event is covered in TAG CNS-TAST-GD-10.2.
- Are there processes to ensure that lessons identified during exercises are incorporated within the SCP?
- Is development, maintenance and review of the SCP subject to appropriate internal assurance processes?
- Are there arrangements to ensure that host police forces and other emergency responders are made fully aware of their part in the SCP?
- Does the SCP adequately address all three phases of an NSE?
- Does the SCP adopt a common lexicon that the SEO and emergency responders can understand (e.g. civil contingencies act lexicon or site based equivalent)?
- Does the SCP adequately address lockdown and personnel accounting arrangements?

- Does the SCP adequately address the dutyholder's response to warning and informing site personnel and to dealing with media interest in a NSE?

19. 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

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

20. GLOSSARY AND ABBREVIATIONS

CCC	Command and Control Centre
CNC	Civil Nuclear Constabulary
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
CT	Counter Terrorism
CTSA	Counter Terrorism Security Adviser
DBT	Design Basis Threat
EOD	Explosive Ordnance Disposal
EP&R	Emergency Preparedness and Response
FSyP	Fundamental Security Principle
GRLS	Government Response Level System
IAEA	International Atomic Energy Agency
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSE	Nuclear Security Event
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
SCP	Security Contingency Plan
SEO	Site Emergency Organisation
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced Person
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
VA	Vital Area

ANNEX A: THE GOVERNMENT RESPONSE LEVEL SYSTEM

ROUTINE

Routine protective measures are to be in place to protect sites and buildings containing NM/ORM and VAs. Should the threat rise additional measures that are appropriate at each location will be required

HEIGHTENED

A Heightened Response Level requires additional protective security countermeasures above NORMAL to address the threat to sites and buildings. Measures deployed should be sustainable indefinitely. They may also be applied as a precautionary measure for a specific period

EXCEPTIONAL

The Exceptional Response Level requires implementation of high levels of protective security measures to minimise vulnerabilities. Extra measures implemented are likely to be sustainable for a limited period only.

.