



ONR GUIDE			
COUNTER TERRORIST CONTINGENCY PLANS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-016 Revision 1		
Date Issued:	January 2016	Review Date:	January 2019
Approved by:	A Cameron	Superintending Inspector	
Record Reference:	2015/311961		
Revision commentary:	Title review		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. REGULATION 4(1) AND 4(3), RELATED REGULATIONS AND INTERNATIONAL RECOMMENDATIONS	2
4. PURPOSE OF NISR REGULATION 4(1) AND 4(3)(D).....	4
5. ADVICE TO INSPECTORS	4
6. FUNCTIONAL AREAS TO BE ASSESSED	7
7. REFERENCES	12
8. GLOSSARY AND ABBREVIATIONS	12

1. INTRODUCTION

- 1.1 The Nuclear Industries Security Regulations 2003 (as amended) (the regulations) (References 1-3) contain requirements for responsible persons to make certain arrangements. The Office for Nuclear Regulation (ONR) inspects and tests compliance with the regulations and associated arrangements to judge their suitability and the adequacy of their implementation. The response to malicious events as defined in Nuclear Industries Malicious Capabilities and Planning Assumptions (Reference 4) and generic threats to Great Britain, includes assessment of the Counter Terrorist Contingency Plan (CTCP), which forms part of the Nuclear Site Security Plan (NSSP).
- 1.2 To support inspectors in assessing the adequacy of such arrangements, ONR produces a suite of guides, which assist the analysis and delivery of regulatory judgements and decisions. This assessment guide, known formally as a Technical Assessment Guide (TAG), is one of the documents provided by ONR for this purpose.

2. PURPOSE AND SCOPE

- 2.1 This TAG contains guidance to advise and inform ONR Security Inspectors in the exercise of their regulatory judgement. It aims to provide general guidance on how to assess the adequacy of a dutyholder's CTCP and is intended to promote a consistent approach to such assessments. It is not intended to be mandatory; rather, it provides a framework on which inspectors can base their judgement during such assessments.
- 2.2 This TAG does not set out how ONR regulates these arrangements, or provide examples of the detailed information a CTCP should contain. These remain the responsibility of the dutyholder and will be site specific.
- 2.3 ONR has provided guidance to dutyholders on completion of CTCPs through the following documents: National Objectives Requirements and Model Standards (NORMS) (Reference 5) and Guidance on Counter-Terrorism Information and Measures for the Civil Nuclear Industry (Reference 6).
- 2.4 This TAG considers the relevant aspects of NISR (Section 3) and identifies their purpose (Section 4). It then provides advice on the assessment (Section 5) and the key considerations which should be reflected in functional areas of the CTCP (Section 6).

3. REGULATION 4(1) AND 4(3), RELATED REGULATIONS AND INTERNATIONAL RECOMMENDATIONS

- 3.1 Regulation 4(1) There must be an approved security plan in place at all times for each nuclear premises (whether or not the premises form part of other premises to which this paragraph applies).
- 3.2 Regulation 4(3) (d) In particular ... the plan must describe the standards, procedures and arrangements relating to - the steps to be taken by the responsible person or any person acting on his behalf if any event of a kind specified in regulation 10(5) (a), (b), (e) or (h) that requires immediate action occurs, and the regular practice of the activities required in connection with those steps.
- 3.3 Regulation 2(1) states that in the regulations, unless the context otherwise requires, nuclear premises means:
- a nuclear site, other than one in relation to which all nuclear material or other radioactive material that was used or stored has been removed as part of the

decommissioning (within the meaning given in Chapter 1 of the Energy Act 2004) of that site

- (aa) a nuclear construction site on which works are being carried out-
 - (i) by a developer; and
 - (ii) pursuant to the grant or issue of a relevant consent, without which the carrying out of those works would be unlawful.
- (b) premises that form part of a nuclear site and are premises on which a person, who is not the holder of the nuclear site licence and is not acting as an officer, employee or contractor of that holder, uses or stores nuclear material or other radioactive material
- (c) other nuclear premises on which Category I/II nuclear material or Category III nuclear material is used or stored, but excluding premises that are used solely for the purpose of the temporary storage of such material during the course of or incidental to its transport in any case where the standards, procedures and arrangements in respect of the security of the transport are contained in an approved transport security statement

3.4 Regulation 2(2) states that the term responsible person, in relation to any nuclear premises, means:

- in the case of a nuclear site falling within paragraph (a) of the definition of “nuclear premises”, the holder of the nuclear site licence
- (aa) in the case of a nuclear construction site falling within sub-paragraph (aa) of the definition of “nuclear premises”, the developer
- (b) in the case of a premises falling within paragraph (b) of that definition, the person mentioned in that paragraph
- (c) in the case of premises falling within paragraph (c) of that definition, the person who uses or stores the Category I/II nuclear material or Category III nuclear material on those premises

3.5 Throughout this TAG the terms responsible person and dutyholder are used interchangeably.

3.6 The events specified in regulation 10(5)(a), (b), (e) or (h) are:

- any unauthorised incursion on to the premises or any attempted or suspected such incursion
- (b) any incident occurring on the premises involving an explosive or incendiary device or suspected such device, or a firearm or replica firearm
- (e) any theft or attempted theft, or any loss or suspected loss, or any unauthorised movement-
 - (i) of any nuclear material used or stored on the premises or in transit to or from them, or
 - (ii) in the case of premises which are or form part of a nuclear site, of any other radioactive material used or stored on them
- (h) any threat to do anything which would fall within any of sub-paragraphs (a) to (g)

- 3.7 The IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 6) deals with planning and preparedness for - and response to - nuclear security events. Under Fundamental Principle K (Contingency Plans), it states:
- Contingency plans to respond to unauthorised 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.
 - Contingency plans should be prepared to counter malicious acts effectively and to provide for appropriate response by guards or response forces. Such plans should also provide for the training of facility personnel in their actions.”
 - These plans (the emergency plan and the contingency plan) should be comprehensive and complementary.
 - The coordination between the guards and response forces during a nuclear security event 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.
 - The operator should initiate its contingency plan after detection and assessment of any malicious act.
 - Contingency plan is routinely reviewed and updated, as necessary.

4. PURPOSE OF NISR REGULATION 4(1) AND 4(3)(D)

- 4.1 Regulation 4(1): The approved security plan is known as the NSSP. It must describe the security arrangements for the nuclear premises as a whole to be approved.
- 4.2 Regulation 4(3)(d): Part of the arrangements for the premises as a whole must describe the standards, procedures and arrangements relating to the steps to be taken in the immediate response to a range of malicious events, and the regular practice of the activities required in connection with those steps. The activities required in connection with those steps are to be adequately described at a high level within the NSSP and in detail by way of a CTCP (Reference 5), which is clearly referenced within the NSSP.
- 4.3 The key clause in relation to a CTCP is the ‘**steps to be taken**’ by the responsible person in responding to malicious events. Additionally, the CTCP should reflect the **regular practice** of the activities required in connection with those steps and the standards, procedures and arrangements contained therein. In part, this regulation 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 Site Emergency Organisation (SEO) functions effectively under potentially hostile and adverse conditions following a malicious event.

5. ADVICE TO INSPECTORS

- 5.1 The purpose of the assessment is to verify that the dutyholder's CTCP provides a framework for the Site Emergency Organisation (SEO) and supports an effective response to malicious events. ONR Security Inspectors will decide whether to validate a CTCP. This section of the TAG will assist inspectors in making that decision. The following information is neither exclusive nor exhaustive, and will be subject to

continual review, but the key features detailed at Section 6 should be found in all CTCPs.

- 5.2 To ensure adequate **'steps to be taken'** are included in the CTCP, Inspectors should seek assurance that all arrangements, including tactics, techniques and procedures, which support the delivery of the CTCP are in place. These could include:
- SEO Training and associated internal assurance reports regarding effective delivery of the CTCP.
 - Any specific written instructions, separate to the CTCP, which support delivery of its OPERATIONAL effect, e.g CNC Local Operating Procedures, building warden instructions or guard force assignment instructions.
- 5.3 Structure of the CTCP
- 5.4 The dutyholder should decide on the content and structure of the CTCP. 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).
 - Guide the decision maker on the actions which need to be taken by the SEO in response to, management of and recovery from a malicious event.
- 5.5 The dutyholder should develop site-specific procedures, as part of the CTCP, to be followed in the event of an incident, or the discovery of something that may cause serious or imminent danger. To ensure compliance, NISR requires all civil nuclear premises to maintain detailed plans which ensure nuclear assets are afforded protection within a CT contingency planning process (including actions to be undertaken when the Government Response Level System is raised). Contingencies should be based on a series of activity lists or checklists to ensure the decision maker understands the actions to be considered by the SEO at each phase of the response. These should be, as follows:

Phase	Objective	Effect
ONE	Immediate response	The OPERATIONAL response of site first-responders ¹ .
TWO	Incident 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 first-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 Home Office Police or Police Scotland.

¹ This can include: CNC, guard force or safety personnel.

- 5.6 **Key characteristics.** Notwithstanding the style or structure of the CTCP, it should have the following attributes:
- Be fully endorsed at Board level or equivalent.
 - Be developed and maintained in accordance with the site quality assurance process.
 - Help provide a rapid response to events by specifying the process and procedure for the assembly and organisation of essential personnel.
 - Identify clear lines of responsibility and associated delegated powers as necessary.
 - Identify the tasks which must be undertaken and achieved.
 - Be delivered by trained and competent personnel at all levels (Suitably Qualified and Experienced Person (SQEP)).
 - Be fully integrated with all appropriate stakeholders, i.e. CNC, Home Office Police/Police Scotland.
- 5.7 Development of the CTCP.
- 5.8 **General.** Heads of Site/Site Directors should select suitably qualified and experienced personnel (SQEP) of appropriate seniority to take responsibility for the preparation, implementation and review of the site CTCP. Such individuals should also form part of the site crisis management planning team, or be familiar with the workings of such a group.
- 5.9 **Liaison.** The CTCP author will need the co-operation of and contributions from other line managers in the site organisation. Liaison with key stakeholders² is also necessary throughout the drafting process. Such activity will ensure the CTCP takes into account, and is complementary to, response plans operated and maintained by each stakeholder. Evidence of such engagement also provides Regulators with assurance that effective working relationships exist.
- 5.10 **Nuclear New Build.** Nuclear New Build sites will require a CTCP to help counter relevant malicious capabilities. Dutyholders must demonstrate a similar level of engagement with key stakeholders during the drafting process.
- 5.11 **Multi-occupancy Sites.** On civil nuclear premises where there is more than one occupier or tenants, and at adjacent nuclear licensed sites, all parties should be aware of the requirement to maintain a CTCP. Periodic joint reviews should be carried out to confirm all parties understand their individual and collective responsibilities. Adjacent or multi-occupant site CTCPs 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 assure Regulators that good working relationships exist.

² Key stakeholders are considered to be: the CNC (where deployed) and/or Home Office Police/Police Scotland, Contract Guard Force /in-house Guard Force and emergency responders, i.e. Fire and Rescue Service and Ambulance Service.

6. FUNCTIONAL AREAS TO BE ASSESSED

6.1 Company Endorsement and Ownership

6.2 **Owner.** The CTCP must be overseen by the Board level member responsible for security.

6.3 **Policy statement.** There should be a clear CT policy statement, which must be endorsed by the Board/Head of Company. The policy statement should recognise the need for a CTCP and acknowledge the requirement for compliance with NISR 2003 (as amended), as 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 CTCP. A site's compliance with the standards in the HMG Security Policy Framework (SPF) (particularly those associated with implementation and use of the Government Response Level System), will be viewed as good practice. SEO personnel are a critical asset within the site response process. Accordingly, if Regulators identified that they would be unable to deliver the plan for any reason, it would be deemed appropriate to withhold validation.

6.4 **Review statement.** In order to confirm their enduring relevance and effectiveness, CTCPs should be included in the annual NSSP review process. This work can be evidenced through the inclusion of a review statement in the NSSP. The review statement should include relevant changes to:

- a. Sector/UK threat and/or response levels;
- b. Site infrastructure/establishment/operations or changes within the site emergency plan/handbook, or key stakeholders plans that are interlinked with the CTCP.

Improvements and/or amendments to the CTCP may be required following exercises, actual events or compliance inspections. CTCPs that are the subject of effective internal audit regimes (verifying the dutyholder and supporting agencies are capable of implementing the CTCP) are more likely to receive regulatory approval.

6.5 **Assurance.** The CTCP should be maintained in accordance with the dutyholders' quality assurance policy and applied consistently to all relevant company sites and areas. The CTCP should also contain details of the roles, responsibilities and positions of those individuals who have quality assured, managed and endorsed it.

6.6 **External partnerships.** The dutyholder (or designated representative such as the Site Security Manager (SSM)) should be able to demonstrate that the CTCP has been developed in partnership with key stakeholders and their endorsement should be evident. A commitment to regular liaison with police Counter Terrorist Security Advisers could also be usefully included (See Para 6.6.2).

6.7 **Distribution.** The CTCP should be controlled and its access restricted to those with a 'need to know'.

6.8 **Command and Control (C2) Arrangements (including command centres, roles, responsibilities and delegated authority).**

6.9 **General.** The dutyholder is required to establish and document within the CTCP, the SEO's roles and responsibilities for determining and implementing appropriate CT security measures.

6.10 **Command Centres.** The purpose, roles and communication structure of OPERATIONAL and TACTICAL C2 nodes should be reflected in the CTCP. Depending on the site function, this could include:

- Emergency Control Centre (ECC).
 - Central Control Room (CCR).
 - Site Security Control Room (SSCR).
 - Security Gatehouse.
 - Police Control Room (PCR) (where CNC are deployed on a site)
- 6.11 **Delegated authority.** Instructions should clearly identify those responsible for performing key tasks when responding to incidents, liaising with emergency first-responders and conducting mandatory notifications, both during and outside of standard working hours.
- 6.12 **CNC.** When developing CTCPs at sites where there is a CNC presence, full consultation is to take place between the CNC and site management (including those with responsibilities for Security, Safety and Emergency Preparedness). This consultation process should ensure CTCPs are coherent, deliver maximum effectiveness, clarify relationships between the 'supported and supporting' commanders and avoid misunderstanding. The CNC Command and Control Centre and Operational Unit Commanders (OUCs), should maintain comprehensive instructions detailing the CNC's response to counter the threats detailed in the NIMCA. It is these response plans which are to be complementary to the CTCP; together they must enable interoperability, unified command and a coordinated and effective response to an incident. There should be evidence that the dutyholder has sought verification that the site's CTCP, CNC response plans, and plans of all relevant emergency first responders, are mutually supportive.
- 6.13 **Interaction with Other Site Plans**
- 6.14 In order to enable interoperability, unified command and a coordinated, effective response to an incident, the CTCP should be harmonised with other site emergency response plans, such as the emergency plan, required under Licence Condition 11, and Emergency Handbook. The CTCP must clearly demonstrate how the decision maker will interface with the company's wider safety, emergency and business continuity planning. There should also be evidence that the author of the CTCP has worked with the authors of both the Emergency Plan and Handbook to ensure all 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.
- 6.15 **CNC.** To assist the decision maker, appropriately sanitised details of CNC actions in support of the SEO response could be included in the CTCP. The inclusion of these details will demonstrate a widespread understanding amongst members of the SEO about the likely tactics, techniques and procedures the CNC could deploy in response to a threat.

6.16 Application of NIMCA Threats, Other Threats and Robustness of the CTCP.

- 6.17 **General.** 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 support a progressive response to a threat. Where Vulnerable Areas are identified on a site, the CTCP should ensure the associated response will prevent an unacceptable radiological release from relevant NIMCA threats. The CTCP should be written in terms which are intelligible to non-security experts, guiding them through the anticipated actions of responders, and outlining relevant secondary hazards.
- 6.18 **Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA).** The CTCP must have contingencies which clearly reflect relevant threat actors to the site, as laid out in the NIMCA document (Reference 5)³. The contingencies in the CTCP should take account of facilities or material which are vulnerable to capabilities outlined in the NIMCA.
- 6.19 **Other threats.** The CTCP reflects any other relevant current generic terrorist or domestic extremist threats to mainland Great Britain. Such threats, even if deemed outside NIMCA, should not be ruled out.
- 6.20 **Robustness.** To ensure the SEO actions are realistic and achievable across the three phases of response, contingency responses should be fully developed, both theoretically and practically. As a general rule, a CTCP which has been validated through desktop exercises, or any other form of drill, and involves all relevant agencies, is more likely to provide effective integrated responses. A CTCP which has been developed purely theoretically cannot be expected to provide the same assurances. Accordingly, evidence of practical development, validation and resulting refinement is more likely to receive regulatory endorsement.
- 6.21 **Guidance and Supporting Information.**
- 6.22 **General.** The CTCP should provide evidence that the importance of CT planning and preparation is appropriately recognised by site senior management. Regulators will seek assurances that it will remain up to date and be reviewed as part of the NSSP review process. Currently, this can be supported as necessary by guidance and advice contained in the ONR document 'Counter Terrorism Information and Measures for the Civil Nuclear Industry' and advice provided by Home Office Police/Police Scotland Counter Terrorism Security Advisers (CTSAs).
- 6.23 **Balance.** The CTCP should not contain an excessive amount of background information or training material to the extent it could hinder navigation by the SEO and their subsequent decision making. Assurances that the SEO and responders are educated 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. minimum cordon distances, briefing templates and supporting mapping, could be usefully included and internally referenced within the Plan.

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 justification for the exclusion of some threats.

6.24 **Liaison and Response with External Agencies including Police CTSAs.**

6.25 **Liaison and Response.** When formulating CTCPs, dutyholders are to establish and maintain links with the local police and other emergency first-responders. When these agencies respond to a site, they will require effective security/technical briefs to highlight the nuclear safety and any other secondary hazard considerations at the site, as well as detail of the ongoing situation. Such briefs will inform the actions of those responders and should their framework should be included in the CTCP. This will help ensure the site identifies and provides whatever is needed for the adequate reception, onward staging and integration of first-responders. Ultimately, the purpose is to ensure the response is integrated and effective, and that command and control is unified.

6.26 **CTSA Liaison.** CTSAs act as a conduit for host police force engagement with dutyholders, contribute to response planning and share good practice. Evidence of engagement with CTSAs will reassure Regulators that the site's response planning has been conducted in concert with Home Office Police/Police Scotland.

6.27 **Site Response Level Arrangements**

6.28 **Overview.** The response level for the civil nuclear industry is based on the Government Response Level System (GRLS). The GRLS is a tiered system against which a range of incremental measures should be applied to counter the threat from terrorism. The site's security regime is to be capable of a rapid and visible adjustment, especially when the response level is raised to quickly counter a change in threat.

6.29 **Response levels.** The GRLS is signified by three stages; NORMAL, HEIGHTENED and EXCEPTIONAL. Each indicates a level of preparedness to counter a threat of terrorism. The response level is determined by the Civil Nuclear Security Intelligence Forum and the range of CT protective security measures applied at each level is a core feature of this system. Accordingly, the CTCP should articulate the site's overall CT posture and the measures to be adopted, as appropriate, for each level. The NORMS GRLS matrix provides useful guidance for dutyholders on generic incremental CT measures to be considered at each response level.

6.30 **Non-nuclear and off-site assets.** For off-site office premises, non-nuclear buildings occupied on licensed sites, and other non-licensed facilities, (particularly those with an obvious association with the civil nuclear industry), a similar approach is strongly recommended to help deliver an appropriate duty of care for personnel. However, for these facilities, the degree of CT protection afforded is for company management to determine.

6.31 **Communication.** Dutyholders must ensure effective communication arrangements are in place so they can respond quickly to any change in the Response Level. This will include briefing staff (including contractors and tenants) on any changes, setting out how such people can seek further information and reiterating their role in supporting the relevant CT response.

Detail. In outline, the CTCP should describe a full range of site-specific incremental measures for each response level. Dependent upon the threat, varying circumstances or local conditions may require the earlier adoption of measures associated with a higher response level, and this should be made clear to the decision maker. In the event of an increase in the response level, the detail within the CTCP should ensure the planned incremental action can be effectively directed and implemented in a timely manner. Generic incremental measures to be applied at the different Response Levels (NORMAL, HEIGHTENED and EXCEPTIONAL) are set out in NORMS (Reference 5).

6.33 Consequence Management

6.34 **Post incident.** The site's primary consideration should focus on ensuring post incident management will not undermine the NSSP. Accordingly, an effective post-incident reporting and review process should be in place.

6.35 **Crime Scene Management.** Following an incident, it may not be possible for the site to operate 'normally' for some time, even if the event caused no damage. Accordingly, the CTCP should provide guidance on the measures that must be taken until police first-responders take responsibility for the scene. This includes:

- a. Maintaining the security of suspected crime scenes;
- b. Preservation of possible evidence;
- c. Security and welfare of witnesses.

6.36 Reporting Arrangements and Media Strategy

6.37 **Reporting.** The plan should detail, in priority order, all mandatory reporting requirements which follow the identification of an event. It should be clear which specific role holder is responsible for reporting and how such reporting should be achieved. It could also usefully highlight those notifications completed by supporting agencies, such as the CNC, in order that the SEO can verify they are complete.

6.38 **Media.** To manage the reactions of site personnel, the public and the media effectively, a media strategy should be included. Designated senior appointments, within the SEO, should also have undertaken media relations training in order to deal confidently with media issues and interviews. If any members of the SEO have undertaken such training, they should be clearly identified within the CTCP as a specific point of contact. The media strategy should be coordinated and agreed with appropriate external stakeholders, such as ONR, DECC and CNC.

6.39 Training Strategy to Deliver SQEP and the Exercising of the Plan in Full

6.40 **Training.** The dutyholder should operate arrangements for training members of the SEO to become SQEP in their roles and able to provide an effective SQEP response at all times. All members of the SEO should be regularly practised and tested on their knowledge and application of the CTCP.

6.41 **Exercising.** The benefits of exercising include the ability to confirm the CTCP is effective against a range of credible events and the verification that members of the SEO, the CNC and other first responders, know their part in it. CTCPs which recognise these (and other) benefits, and put them into practice, will be readily approved by the Regulator. Exercises can be desktop or live-play and can test many facets of the site response. The plan should be exercised regularly and, if necessary, updated to maintain an adequate level of response. All protective security measures applied to protect NM/ORM and VAs from sabotage and theft should, at some point, be exercised. Furthermore, malicious events that are identified in the CTCP should be specifically covered within the exercise programme over time. Exercising may also lead to targeted training if it identifies that personnel would benefit from more knowledge or practice of particular aspects. The scope of exercises is very broad. The exercise might be simple, desk-based and have limited objectives, such as verifying that the extra measures to be applied at a higher response level can be implemented. Conversely, it might take the form of a fully assessed live-play involving all supporting agencies.

6.42 **Post-Exercise Reviews.** The benefit of conducting thorough post-action reviews of exercises should be reflected in the CTCP. Such reviews typically identify good

practice and areas for improvement. The latter should be used to improve the CTCP, and by association the SQEP of the SEO and other key staff/responders, and the mechanism for doing so should be clear.

- 6.43 **Audit.** All training activity associated with delivery of the CTCP, be it individual or collective, should be recorded within the dutyholder's wider general assurance regime.

7. REFERENCES

1. Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403
2. Nuclear Industries Security (Amendment) Regulations 2006. Statutory Instrument 2006 No. 2815
3. Nuclear Industries Security (Amendment) Regulations 2013. Statutory Instrument 2013 No. 190
4. Nuclear Industries Malicious Planning Capabilities and Planning Assumptions.
5. National Objectives, Requirements and Model Standards. Issue 2: April 2014. Trim Folder 4.4.2.13778.
6. Guidance on Counter Terrorism Information and Measures for the Nuclear Industry. Issue No 1: March 2012.
7. The IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities. (INFCIRC/225/Revision 5).
8. ONR: Classification Policy for the Civil Nuclear Industry: Version 7

8. GLOSSARY AND ABBREVIATIONS

C2	Command and Control
CGF	Civilian Guard Force
CNC	Civil Nuclear Constabulary
CT	Counter-Terrorism
CTCP	Counter-Terrorism Contingency Plan
GSC	Government Security Classification
JESIP	Joint Emergency Services Interoperability Programme
JTAC	Joint Terrorism Analysis Cell
MACP	Military Aid to Civil Powers
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material

OUC	CNC Operational Unit Commander
SEO	Site Emergency Organisation
SSM	Site Security Manager
SQEP	Suitably Qualified and Experienced Personnel
VA	Vital Area