1

ONR GUIDE			
CLARITY OF COMMAND, CONTROL AND COMMUNICATIONS ARRANGEMENTS DURING AND POST A NUCLEAR SECURITY EVENT			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-10.3 Revision 2		
Date Issued:	October 2020	**Review Date:**	October 2021
Approved by:	Matt Sims	Professional Lead	
Record Reference:	CM9 Folder 4.4.2.23373. (2020/273838)		
Revision commentary:	Fit for Purpose Review of Rev.1 Inclusion of Joint Services Interoperability Programme (JESIP) terminology at 7.3.		

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 Command, Control and Communications (C3) arrangements and infrastructure. 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 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.

4.3 The importance of issues relating to command and control during 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 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 an 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). Sections 4 and 5 of this document contain specific measures for armed response forces in the prevention of theft or sabotage against nuclear facilities and nuclear material in use and storage. Paragraph 4.15 states that provision should be made for detecting unauthorised intrusion and for appropriate action by enough guards and/or [armed] response force to address a nuclear security event.

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 10.3 – Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event, 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 An effective response to a NSE is dependent on a dutyholder's Site Emergency Organisation (SEO) infrastructure and capability to support clarity of C3 arrangements throughout the event. The three phases of a NSE can be described as:

Phase	Objective	Effect
ONE	Immediate response	The OPERATIONAL[1] response of site first-responders to a nuclear security event.
TWO	Event management	The integrated TACTICAL[2] management of a nuclear security event up to the threat being neutralised/ risk reduced to 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 (where deployed) and/ or Host police forces. Conduct of liaison with an off-site multi-agency STRATEGIC[3] coordination group.

6.1 The response should be integrated and involve all relevant stakeholders at each phase of the NSE and it is important that the response is supported by robust and resilient command nodes. The resilience should be designed to mitigate an unacceptable interruption or loss of capability, including that which may be caused by malicious attack. Such infrastructure resilience will provide confidence that all systems and personnel can function effectively and that communications to enable information and instructions to be transmitted across the SEO and its stakeholders on, and where necessary off the site, remain available.

Regulatory Expectations

6.2 The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how C3 infrastructure and arrangements can support an effective response.

[1] OPERATIONAL: The management of 'hands-on' work undertaken during the nuclear security event.
[2] TACTICAL: The level of command above OPERATIONAL of the site response to a nuclear security event.
[3] STRATEGIC: The level of command above TACTICAL where policy, strategy and an overall response framework is established and managed.

FSyP 10 - Emergency Preparedness and Response	Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event	SyDP 10.3
Dutyholders should implement structures and processes to ensure effective command, control and communications arrangements during and post nuclear security events.		

7. ESTABLISHMENT OF ROBUST AND RESILIENT COMMAND, COMMUNICATIONS AND CONTROL ARRANGEMENTS

7.1 The dutyholder should identify and implement a structured network of command nodes to enable the delivery of an effective response to a NSE. These should:

a. direct the OPERATIONAL and TACTICAL elements of the SEOs response to an NSE; and,

b. enable liaison with any off-site multi-agency STRATEGIC command groups, whenever required.

Command Nodes

7.2 Depending on the category of the site, the C3 strategy should include command nodes that direct the OPERATIONAL and TACTICAL aspect of the SEO response. Depending on the category of the site, these could include the following:

Command node	Command Effect	Command purpose
Site Security Control Room (SSCR)	OPERATIONAL	• Monitor and control all on-site security activities. • Delivers situational awareness to first responders. • Directs and communicates with the site response force. • Subordinate to TACTICAL command nodes.
Alternate SSCR	OPERATIONAL	• Delivers the function of the SSCR when it is not operational for any reason. • It should replicate the purpose and effect of the SSCR.
Central Control Room (CCR),	TACTICAL	• Command and control of the site response by the site's duty Duly Authorised Person (DAP) in

Access Control Point (ACP).		concert with CNC OPERATIONAL commanders (where deployed). • Communicates with OPERATIONAL command nodes. • If the site is required to have an Emergency Control Centre (ECC), the DAP will handover command to the ECC/Alternate ECC once established (normally after the **immediate response** phase). However, it must have the capability and be prepared to, maintain command if the ECC/AECC cannot operate.
Police Control Room (PCR) (where established).	OPERATIONAL	• Delivers situational awareness to CNC first responders. • Depending on the site, could be subordinate to the CNC Force Incident Manager (FIM), based at the CNC Command and Communication Centre (CCC).
Emergency Control Centre (ECC)	TACTICAL	• Command and control of the integrated (safety and security) SEO response to deliver the **event management** and **consequence management** phases of a NSE. • Commanded by the site's senior duty DAP in concert with CNC FIM (where appropriate).
Alternate ECC	TACTICAL	• Delivers the function of the ECC when it is not operational for any reason. • It should replicate the purpose and effect of the ECC.
Centralised Command Facility (CCF)	OPERATIONAL AND TACTICAL	• Contains the SSCR, ECC and PCR function. Either liaises with/or subsumes the CCR/ACP function. Commands **all three phases of the site response** to a nuclear security event. • Commanded by the site's senior duty DAP in concert with CNC FIM (where appropriate).

From a security responder perspective, key command nodes are the SSCR, PCR and CCF.

Command Policy

7.3. Within the site Security Contingency Plan (SCP), the dutyholder should:

a. Define command node roles and relationships.

b. Through a memorandum of understanding (or equivalent) Identify stakeholders who will undertake the lead organisation responsibilities in delivering a response to an NSE. Each stakeholder should understand each other's legal responsibilities and obligations.

c. Describe the roles and responsibilities of commanders and subordinate personnel.

d. Ensure key command nodes are, as appropriate, staffed by Suitably Qualified and Experienced Persons (SQEP) personnel at all times during routine operations and a NSE.

Resilience

7.4. Dutyholders should ensure that all command nodes are:

a. Resilient to any unacceptable interruption or loss of its function due to, for example, the loss of security technology, communications or key utilities whether on or off-site.

b. Capable of sustaining personnel for the time it takes to deal with an NSE, including the consequence management phase.

c. Supported by enough SQEP personnel to relieve command node staff whenever required, particularly during a protracted event.

Communications

7.5. Dutyholders should have a communications strategy that:

a. Enables all elements of the SEO to communicate effectively and deliver a timely response to a NSE at all times.

b. Supports external stakeholder's activities in respect of their C3 integration with the SEO response to a NSE.

c. Provides the CNC, where deployed or established, with a communication system capable of supporting all their tasks whether on or off site.

d. Prevents any adverse impact on key safety or security systems.

e. Includes an assurance process that tests and maintains the system to ensure a site's response to an NSE is effective.

8. COMMAND, CONTROL AND COMMUNICATIONS INFRASTRUCTURE

Security

8.1 Command nodes should have physical and protective security measures that are adequate and proportionate about achieving the required Physical Protection System (PPS) outcome. Other factors for consideration may include:

- Any weapons systems or ammunition stored therein and their availability.
- The security classification of information or apparatus held within it.
- The anticipated response times from both on and off-site security responders.

Ergonomics

8.2 Each command node should have enough space, equipment and furniture to concurrently enable:

- Staff and stakeholders to undertake individual or collective activity effectively.
- The operation of all information, communication and technology systems and associated apparatus so that the command node can always deliver its function.

Inspectors should consider:

- Are there appropriate arrangements for C3 to be maintained throughout all phases of emergency response?
- Is there an appropriate structured network of command nodes to enable delivery of an effective response?
- Does the Security Contingency Plan (SCP) plan define the command node roles and relationships?
- Does the SCP identify lead-coordination agency stakeholders and describe the roles and responsibilities of commanders and subordinate staffs?
- Are the command nodes staffed by SQEP personnel?
- Are the command nodes resilient to loss of function (e.g. utilities) and capable of being staffed continuously, including for protracted NSEs?
- Are communication arrangements and command node functions appropriately tested?
- Are the command nodes afforded appropriate physical protection to ensure that the required PPS outcome is achieved?
- Are the interiors of the command nodes ergonomically designed to support delivery of the required functions at all times?
- Does the dutyholder adopt a common lexicon that can be understood by all SEO agencies and emergency responders?

9. 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.

10. GLOSSARY AND ABBREVIATIONS

ACP	Access Control Point
AECC	Alternate Emergency Control Centre
C3	Command, Control and Communications
CCC	Constabulary Communications Centre
CCF	Centralised Command Facility
CCR	Central Control Room
CNC	Civil Nuclear Constabulary
CNS	Civil Nuclear Security
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
DAP	Duly Authorised Person
ECC	Emergency Control Centre
FIM	Force Incident Manager
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
PCR	Police Control Room
PPS	Physical Protection System
SCP	Security Contingency Plan
SEO	Site Emergency Organisation
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SSCR	Site Security Control Room
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide