ONR GUIDE			
SECURITY DECISION MAKING			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-1.3 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19071. (2017/100006)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/17

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 decision making processes. 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 leadership and management for security 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 Principle K of the CPPNM refers to the production of contingency plans to respond to unauthorised removal of nuclear material or sabotage of nuclear

facilities. The importance of being able to respond, and respond effectively is reinforced by Essential Element 11: Planning for, preparedness for, and response to, a nuclear security event, specifically – 3.12 a) Developing arrangements and response plans for ensuring rapid and effective mobilisation of resources in response to a nuclear security event; and, effective coordination and cooperation.

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).

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 1.3 – Decision Making, in support of FSyP 1 – Leadership and Management for Security. 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 Nuclear security decision-making encompasses a wide span of activity. It takes place at all levels within an organisation from the operational to the strategic. At the operational level some decisions could be time critical, largely based on intuition and taken by relatively junior personnel based on less than perfect situational awareness[1]. Some strategic security decisions could take months to make, require careful analysis of a wide range of factors and the establishment of consensus with internal and external stakeholders. Recognising the breadth of activities covered by this TAG only general guidance from ONR is provided to assist inspectors when assessing particular aspects of decision making by dutyholders.

Regulatory Expectation

6.2 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan details how decisions with the potential to affect security are taken using a prudent, rational process that incorporates diversity, transparency and challenge.

[1] Defined as what is happening at a particular time and place that may affect the site's security

FSyP 1 - Leadership and Management for Security	Decision making	SyDP 1.3
Decisions made at all levels in the organisation affecting security should be informed, rational, objective, transparent and prudent.		

Decision-making

6.3 Any nuclear security decision making process must enable prudent, timely decisions to be made at the appropriate level by Suitably Qualified and Experienced Persons (SQEP) personnel; however, they must also permit decision-making to be transferred elsewhere within the organisation, if the situation requires it. Dutyholders should not require all security decisions to be 'referred upwards', but senior managers should be involved in making strategic-level security decisions (the appropriate involvement of senior managers, individual directors and the governing board in strategic-level security decisions should be expected).

6.4 Security related decisions should also cater for the potential for error, uncertainty and the unexpected, and those taken in the face of uncertainty or the unexpected should be appropriately and demonstrably conservative. In particular, operational decisions may have to be made quickly, with imprecise and incomplete information.

6.5 Security-related decisions should not be 'out-sourced' to a third party, such as contractors. However, where appropriate, decision making should incorporate diversity of view, for example by involving individuals from other business units in the peer review process.

6.6 Where civilian guard forces are utilised and their shift supervisors and junior managers are authorised to make operational decisions, their authority should be bounded and subject to appropriate oversight by SQEP personnel and their decisions should be suitably prudent and conservative.

Decision-makers

6.7 Decision makers should be able to obtain appropriate situational awareness and understanding, engage effectively with stakeholders, listen to the advice of SQEP and develop alternative potential options. Decision makers should have the necessary organisational authority to make the required decisions and the means to ensure that their decisions are implemented. At the operational level decision-makers should have the opportunity to learn and practice decision-making processes under realistic conditions within the context of the Design Basis Threat (DBT).

6.8 Decision makers should be able to demonstrate that they can make balanced, rational decisions that take account of identified vital areas and associated hazards, the likely operational impacts of decisions, any safety needs, the graded approach to security, and the needs of the business. Unqualified, inexperienced or temperamentally unsuitable personnel should not be in roles where they will be required to make significant (and/or time-critical) security related decisions. Inexperienced decision makers should be supported through a structured programme of training/mentoring.

Situational Awareness & Understanding

6.9 There should be sufficient numbers of SQEP personnel within an organisation's security staff who can understand the broader context that will affect security related

decisions, identify potential solutions to problems and advise senior decision-makers within an organisation. This should not be 'out-sourced' to contractors. Decisions should be based on the best available information within the timescale for the decision being necessary. At the operational level this may be reliant on ensuring that decision-makers have appropriate local knowledge of a site, situational awareness and required security responses. At the strategic level this may require decision-makers to understand the broader context (including potential constraints) that could affect security related decisions and what is needed to achieve a solution. This could include:

- Why a decision is required and the potential risks and benefits associated with it.
- The desired security outcome(s).
- Nuclear Safety requirements and constraints.
- Conventional health and safety.
- Emergency planning and response.
- Comprehensive knowledge of all aspects of nuclear security 'good practice' including, where applicable, the CNC's role and concept of operations (or similar where the response is provided by the local police force).
- Knowledge of the DBT.
- Detailed knowledge of all security risks and vulnerabilities at a site or sites.
- Understanding the potential benefits and limitations of security technology.
- The needs of the business.
- Resourcing requirements.
- Legal requirements.
- Regulatory requirements and expectations.
- Potential reputational impacts.

Stakeholders

6.10 Internal and external stakeholders should be identified and involved in the decision-making process where appropriate and when time allows. Decision-making processes, at both the operational and strategic levels, should enable stakeholders to be easily identified and informed. At the strategic level key internal stakeholders could include the senior information risk officer, senior business managers and directors. Key external stakeholders could include the CNC and the civil police.

Developing/Testing Options

6.11 Where time allows potential options that could achieve the desired outcome should be developed and tested. There is rarely only one possible solution to a particular problem or issue that requires a decision. Potential alternative options should be developed and assessed or tested to ensure that they can achieve the required outcome within any

identified constraints. Options should be assessed or tested utilising SQEP personnel who are independent from the individual or group that developed them.

Accountability & Auditability

6.12 Designated individuals within the organisation should be accountable for the security decisions that are made and the actions that are subsequently taken (or not taken) because of them. Individual responsibility for security decision-making should not be outsourced, diluted or concealed. The decision-making process should be suitably transparent auditable and relevant records kept for an appropriate period of time (depending upon the nature and outcome of any decision).

Consistency & Simplicity

6.13 Organisations should use consistent and simple decision-making processes and methodologies that aid decision-makers. The processes should avoid unnecessary complexity and bureaucracy, and enable them to make appropriate decisions in the time they have available to achieve the desired outcome. The CPNI Operational Requirement process (or similar) is one potential option to identify physical security requirements, constraints and potential solutions.

Reassessment & Learning

6.14 Organisations should demonstrate that they are sufficiently flexible to reassess decisions and amend potential solutions if relevant factors change to the extent they could affect the desired outcome (such as the identification of new assets, vulnerabilities or the changing nature of the threat). Decision-making processes should also demonstrate the ability to assimilate relevant good practice and learn from the experiences of others.

Challenge

6.15 Active challenge should be part of decision-making throughout the organisation including at Board and senior management levels. The organisation should encourage a questioning attitude from all staff and contractors. Though the form and function of the challenge will vary between different areas and levels within organisations, designing-in appropriate active challenge mechanisms should be an inherent part of all decision making processes affecting security. Active challenge should:

- occur routinely as a result of a questioning attitude in the culture of staff and contractors;
- occur by design, and transparently, in all key decision making processes that may affect security;
- not originate solely from independent security assessment or peer review;
- assume that failure through inadequate design or implementation is possible, and be proactive in looking for ways that things could go wrong;
- be applied to technical/facility-based and management decisions; and
- be used in operational decision making in normal, threat and security event situations (subject to the need for security related decision-making to be suitably timely and appropriate).

Organisational Behaviours

6.16 Organisations should demonstrate that security related decisions are not negatively influenced by behaviours such as: group-think, bias and organisational culture (particularly behaviours that could encourage complacency about security related decisions – such as a belief amongst decision-makers that 'it could never happen here' or underestimating a potential adversary).

Inspectors should consider:

- Does the process enable prudent and timely decisions to be made at the appropriate level by competent personnel?
- Do decision-makers have the necessary authority and the means to ensure that their decisions are implemented?
- Are decision-makers demonstrably able to make rational, prudent and timely decisions?
- Are inexperienced decision-makers suitably trained and mentored and do they have the opportunity to realistically, but safely, practice their decision-making skills and learn from the experience?
- Are there processes to ensure that senior decision-makers are provided with adequate situational awareness and understanding to ensure that decisions are informed by the best available information in the time at hand?
- Are there mechanisms in place to, where appropriate, involve internal and external stakeholders in the decision making process?
- Where time is available to do so, does the decision-making process allow for a range of potential solutions to be developed and tested?
- Is the process appropriately transparent, auditable and require designation of individuals who are accountable for decisions taken?
- Does the process employ consistent, simple processes and methodologies that assist decision-makers?
- Is the process adequately flexible to allow for reassessment of decisions and incorporate learning?
- Is the process protected from negative influences and behaviours and allows for appropriate challenge?

7. 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/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

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

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

8. GLOSSARY AND ABBREVIATIONS

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
L&MFSy	Leadership and Management for Security
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
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