ONR GUIDE			
SECURITY GUARD SERVICES			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-9.3 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19080. (2017/110576)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's Civilian Guard Force (CGF) 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 policing and guarding 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). 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. In particular, paragraph 4.15 states that provision should be made for detecting unauthorised intrusion and for appropriate action by sufficient guards and/or [armed] response force to address a nuclear security event.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 9.3 – Security Guard Services in support of FSyP 9 – Policing and Guarding. 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 premises should have a CGF (either 'in house' or contract). The level and capability of the CGF response should be appropriate to achieve the required security outcome as detailed in FSyP 6 – Physical Protection Systems (PPS). The CGF must appropriately integrated and co-ordinated with other aspects of the PPS and the CNC (where deployed).

6.2 This TAG informs regulatory assessment of the dutyholder's policing and guarding arrangements and in particular the integration of the dutyholder's security regime and the civilian guard force.

Regulatory Expectation

6.3 The regulatory expectation is that the dutyholder demonstrates within their security plan how they implement and maintain CGF operations that are fully integrated with relevant stakeholders and the PPS to ensure the required security outcomes are achieved.

FSyP 9 - Policing and Guarding	Security Guard Services	SyDP 9.3
Dutyholders should employ civilian security guards to provide the unarmed guarding that conducts nuclear security operations as described in the site security plan such as patrolling, access control and searching; and, who deliver or enable the immediate response to a security event.		

7. ESTABLISHING A CGF

7.1 Dutyholders are responsible for creating a CGF structure and concept of operations in order to deliver the PPS outcomes for the site and/or material being protected. In designing the PPS, views of key stakeholders (for example the CNC and local police force) should be taken into account along with the current threat and malicious capabilities postulated in the extant Nuclear Industries Malicious Capabilities Planning Assumptions document.

7.2 Once a decision on the numbers and disposition of the CGF has been made the detail is to be included into security plans. Any proposed alteration to CGF operational activities that has the potential to affect the dutyholder's ability to achieve the required security outcome should not be implemented until the revised arrangements have been approved in an amendment to the security plan.

7.3 Although dutyholders may vary the hours worked by security staff in their employment to permit part-time and flexible working, including job-sharing, there should be appropriate and available CGF cover to ensure an appropriate response to any security events, warnings or changes in the Government Response Level System.

7.4 The CGF on nuclear premises can consist of in-house fulltime employees or be provided through a contract service provider. Inspectors should apply this TAG equally to both types of guarding.

7.5 Proposals to utilise mixed-force arrangements at sites, for example contract CGF working with directly employed guards, should be described in the approved security plan, and agreed in advance by ONR. This is to allow management arrangements to be assessed to ensure that management and control problems will not arise when responding to security incidents.

7.6 The dutyholder should define the roles and responsibilities of the CGF in security plans (including security contingency plans) and that designated CGF managers and supervisors should be appropriately trained, experienced and capable.

7.7 The dutyholder should ensure that the CGF members hold appropriate National Security Vetting (NSV) for their roles. Where guards are not cleared, or whose clearance is under review, ensure they do not have access to sensitive areas or equipment unless under escort.

7.8 The dutyholder should articulate CGF roles and responsibilities in security working instructions (SWIs) or Assignment Instructions (AIs) and these should be underpinned by robust company security policies and procedures.

7.9 The dutyholder should identify future requirements for CGF including resourcing, recruiting, training and equipping.

8. CGF SUPPORT TO NORMAL OPERATIONS AND EMERGENCY RESPONSE

8.1 The dutyholder should ensure sufficient resource is available to meet the requirements of the approved security plan. This applies to normal site operations over a 24/7 cycle and has in place contingencies to generate increased staffing levels to meet Site Emergency Operations (SEO).

8.2 The CGF should be an integrated force, able to carry out the physical demands of the job and duties within the site's command and control structure. There should be effective command and control for all CGF operations on site to facilitate an appropriate response to all security events that achieves the required security outcome. This may include supporting/facilitating an armed response force in the delivery of effective and proportionate countermeasures to the relevant malicious capabilities outlined in the extant NIMCA document.

8.3 The CGF should be capable of effectively managing access control and identifying/reporting suspicious activity and anomalies. This includes attempts to introduce prohibited items to the site or the unauthorised removal of NM/ORM or SNI.

8.4 The CGF should be capable of co-ordinating/de-conflicting its activities with the CNC/local police (where appropriate).

9. TRAINING AND EXERCISING A CGF

9.1 The dutyholder should ensure that the CGF is appropriately trained in their roles and responsibilities. Training packages should be applicable to normal and emergency situations, and will align with the SEO requirements. Training records for individual members of the CGF should be maintained. Dutyholders should implement a demonstrably effective exercise regime that provides realistic and challenging scenarios for all members of the CGF (in conjunction with the CNC and local police where appropriate).

10. CGF EQUIPMENT COMMUNICATIONS AND SITUATIONAL AWARENESS

10.1 The dutyholder should ensure that the CGF has appropriate personal equipment and vehicles to perform their duties as detailed in the security plan. The CGF should also have robust and secure communications across the site enabling the CGF to communicate effectively with CNC/local police (if appropriate) and members of the SEO in all situations. The dutyholder should also ensure that important, timely and relevant information is provided to the CGF, enabling them to assess and respond

effectively to security incidents and co-ordinate their response with CNC and the local police.

11. FUNCTIONAL ASSURANCE – 'IN-HOUSE' CGF

11.1 The dutyholder should establish Key Performance Indicators (KPI) for the security function of the CGF, including CNC/local police liaison (where appropriate) to meet the requirements of the security plan. The dutyholder should also ensure that the CGF's security functions are assessed by the internal assurance staffs at least annually.

12. FUNCTIONAL ASSURANCE – CONTRACT CGF

12.1 The dutyholder should ensure that the contracted CGF meets all its contractual obligations to support achievement of the security plan and can demonstrate this through clearly defined KPIs and written agreements. If a contract CGF cannot meet its contractual requirements there should be arrangements in place to ensure that the contract CGF improves its performance or can be replaced without affecting the delivery of the security plan.

13. RESILIENCE

13.1 The dutyholder should ensure that there are appropriate arrangements in place to ensure that all essential CGF security posts and roles can be appropriately staffed at all times. The duty holder should ensure that contingency plans (referenced in the security plan an appropriately exercised) describe the arrangements for addressing the effects on a CGF of: staff sickness, adverse weather conditions and industrial action.

Inspectors should consider:

- Does the CGF have sufficient capability and capacity to deliver the functions detailed in the PPS and achieve the required security outcome?
- Are CGF roles and functions appropriately articulated within the security plan?
- Is the CGF appropriately integrated with other aspects of the PPS and CNC?
- Is the CGF appropriately managed and supervised?
- Is the CGF appropriately trained and exercised in the roles and functions they perform?
- Is the CGF appropriately equipped to perform all its functions in the security plan?
- Are CGF staff appropriately vetted and supported by the dutyholder's personnel security processes and procedures?
- Are CGF staff physically able enough to undertake their roles and functions?
- Are there arrangements to ensure the CGF can communicate effectively with the CNC, local police and adjacent sites and other stakeholders?

- Are the CGF's activities appropriately managed, assessed and assured against KPIs and written agreements?
- Are there mechanisms in place to mitigate/improve individual or collective under performance by the CGF?
- Are there appropriate contingency plans to ensure that CGF roles and functions are appropriately resilient?
- Are future requirements for CGF appropriately identified and resourced?

14. 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. 2017/124772

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

15. GLOSSARY AND ABBREVIATIONS

AI	Assignment Instructions
C3	Command, Control and Communications
CGF	Civilian Guard Force
CNC	Civil Nuclear Constabulary
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
KPI	Key Performance Indicator
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
NSV	National Security Vetting
ONR	Office for Nuclear Regulation
PPS	Physical Protection System
SEO	Site Emergency Operations
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SWI	Security Working Instructions
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide