Procedures and Administrative Controls			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-3.4	**Issue No.:**	3
Record Reference:	2022/15396		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Principal Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	Major update to align with updated SyAPs.		

Table of Contents

1. Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.

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. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR 2003') [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] 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 TAG is such a guide.

2. Purpose and Scope

3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's procedures and administrative controls. 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 UK Legislation and Policy

4. 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.

5. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR 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 CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

6. 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 3.4 – Suitable and Sufficient Procedures and Administrative Controls, in support of FSyP 3 – Management of Human Performance. The TAG is consistent with other TAGs and associated guidance and policy documentation.

7. The Government Functional Standard on security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within the Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

8. The Government Security Classifications document, together with the ONR Classification Policy [4] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

4. Relationship to International Standards and Guidance

9. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals [6]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

10. Fundamental Principle E of the CPPNM refers to the responsibility of dutyholders to implement a Physical Protection System (PPS). It details that the State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorising documents.
The importance of physical protection of Nuclear Material (NM) and Other Radioactive Material (ORM) is also recognised in the Nuclear Security Fundamentals, specifically Essential Element 3: Legislative and Regulatory Framework – 3.3.

11. The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime should provide for the establishment of systems and measures to ensure that NM and ORM are appropriately accounted for or registered and are effectively controlled and protected.

12. Fundamental Principle I of the CPPNM refers to the concept of several layers and methods of protection (structural or other technical, personnel and organisational) afforded by the PPS. A more detailed description of the graded approach is provided in Recommendation's level guidance, specifically Nuclear Security Series (NSS) 13 [7]. This document states that dutyholders should prepare a security plan based on a threat assessment or the design basis threat and should include sections dealing with design, evaluation, implementation, and maintenance of the PPS. Sections 4, 5 and 6 contain more detailed guidance on specific measures that dutyholders should adopt to protect NM/ORM against theft and sabotage.

13. The importance of issues relating to human performance are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:
    - d) Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear security responsibilities on a continuing basis using a risk informed approach; and
    - e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the nuclear security systems.

14. A more detailed description of the elements is provided in Recommendations level guidance, specifically NSS 13 [7]. This publication highlights the importance of designing robust Physical Protection Systems including engineered and operational security measures, evaluating and demonstrating their effectiveness. It also highlights the importance of ensuring integrated solutions that manage the interface with safety systems to avoid adverse impact and to ensure they are mutually supportive.

5. Advice to Inspectors

15. Humans play a key role in the delivery of nuclear security, forming an integral part of the physical protection system and cybersecurity and information assurance arrangements. Where tasks are undertaken by people in support of nuclear security, the way in which these are completed should be prescribed by well-designed and well written procedures. Within this guidance the term procedures is used to encompass all written instructions that describe the way in which tasks affecting security should be performed. This can include security operating procedures, alarm response instructions, maintenance instructions pertaining to engineered systems necessary for the delivery of security, as well as management procedures, for example those relevant to maintenance of personnel security vetting.

16. Where the achievement of security functions is dependent on human based processes, these processes are identified as administrative controls. Examples of administrative controls in the security context include:

- where access to a site or specific area of a site is controlled by security personnel and is dependent on confirming the identity of authorised personnel and visitors before access is granted,
- arrangements to control and monitor the movement of NM/ORM using accountancy and safeguards and procedures,
- Escorting of staff, contractors or other visitors who require access to site or specific areas thereof for which they do not have authorisation for uncontrolled access.
- The use of patrols and monitoring in situations where Closed Circuit Television (CCTV) cameras may be unavailable, e.g., due to maintenance, to detect attempted intrusion onto a site.

17. In order to ensure that administrative controls are designed to maximise human performance, it is important that these are analysed and tested, and that evidence of their effectiveness in the provision of security is provided in the dutyholder's security plan and supporting documentation.

18. This TAG informs regulatory assessment of the management of human performance and addresses the aspects of procedures and administrative controls.

19. This guidance should be applied in a proportionate and targeted manner at each stage of a system's lifecycle. The emphasis that the inspector gives to assessing different elements of a dutyholder's arrangements and outputs in the form of procedures and administrative controls will depend upon the plan being assessed and the graded approach. For example, where the procedures and administrative controls are already well established and there is good evidence of successful performance using them, it may not be

necessary to closely scrutinise them. Conversely, where new activities are being developed or wholesale changes are made to the arrangements for the development or management of procedures and administrative controls, then closer examination may be warranted. As an overriding principle, the inspector should consider the security significance (such as the security function category or the categorisation for theft or sabotage) of the activities concerned and the relative contribution of the human for the delivery of security.

6. Regulatory Expectation

20. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies how they adopt a systematic approach in order to provide suitable and sufficient procedures and administrative controls to support people in the delivery of nuclear security.

FSyP 3 – Management of Human Performance	Suitable and sufficient procedures and administrative controls	SyDP 3.4
Dutyholders should demonstrate that sufficient procedures and administrative controls are provided, which are designed to minimise the likelihood of human error and support reliable delivery of security functions.		

7. Procedures

21. All activities which may affect nuclear security should be carried out in accordance with written procedures. However, carrying out activities in accordance with procedures does not necessarily mean that there must be a procedure in hand, followed step by step for every task. Decisions on the way that procedures are used to support consistent and reliable task performance must be based on the nature of the task, its security significance, the potential for error, and the experience and training of the user.

22. Dutyholders' management arrangements for procedures should stipulate how procedures are intended to be used during task completion, this may be in the form of a procedure classification system. In the nuclear industry it is common that procedures are classified for use at three levels, based on the importance of the task, its complexity and how often it is performed. A typical procedure classification system uses the following use categories:

- Continuous use – Procedures are used in hand at the point of work and each step is recorded as it is completed.
- Reference use – The procedure is present at the point of work and is referred to as required. Completion of sections of a procedure may be recorded.
- Information use – The procedure should be available to be used at the point of work if required. A record that the procedure has been followed may be made, this may be in the form of confirmation that an entrant to a restricted area has had his or her identity formally confirmed.

23. Procedures should document the way in which tasks are required to be performed and users should recognise the importance of adherence to them. Dutyholders should have arrangements in place to demonstrate that procedures are used in the way intended and are adhered to at all times. Managers and supervisors play an important role through appropriate oversight and in ensuring procedure use and adherence. Evidence of the effectiveness of this should be collected by dutyholders. This forms part of, and provides evidence for, a robust security culture.

24. It is important that a dutyholder's arrangements in relation to procedures provide a controlled and effective process for the production, maintenance, review, amendment and version control of procedures. Importantly, the arrangements should detail the process by which users are informed of procedure amendments and ensure that all users understand and comply with the amended requirements.

25. The dutyholder's process for the production and amendment of procedures should include a process of verification and validation to ensure that procedures are technically accurate; can be used as intended at the point of

work; and are fully understood by end users. In some cases, it may be appropriate that procedures are designed on the basis of a formal task analysis process. It is noted that procedures benefit from the involvement of end users during their development. Procedure verification and validation can be undertaken as a tabletop exercise or by conducting a walkthrough of it at the point of work. The dutyholder's arrangements for the production of procedures should specify when different forms of verification and validation exercises are required.

26. The dutyholder's organisational arrangements should clearly identify those with roles and responsibilities for the development and maintenance of procedures, and adequate resources should be provided for these roles. These organisational arrangements should include both dedicated resources for procedure production and management, including version control of procedures, as well as more ad hoc resources e.g., access to personnel from other disciplines who can contribute timely review and validation and verification of procedures. The organisational arrangements should allow for an effective and efficient process by which procedure users can identify the need for procedure updates. It is important for procedural use and adherence that users perceive procedures to be accurate and rapid update in response to identified shortfalls is an important component of this.

27. Procedures should be developed according to dutyholder arrangements that specify how procedures should be presented, the level of detail to be contained within procedures of different types, the structure and language used for the presentation of task steps and how task completion is recorded. Dutyholders may consider the development of a procedure writer's guide to ensure consistency in the format and presentation of procedures and training to enhance understanding of this and consistent application. Consistency is important as a means of reducing error and improving human performance.

28. The dutyholder should also demonstrate learning from experience, for example implementing appropriate improvements following events, feedback from personnel following use during operation, training, drills, and also from cross-dutyholder comparisons.

29. Whilst consistency in procedure format and presentation has benefits, it is likely to be the case that different formats are required for procedures of different types. For example, procedures governing task completion for normal security operations such as the conduct of searches are likely to be different to those directing operations during security events. These are also likely to differ in format and content for maintenance activities undertaken on security equipment. Thus, dutyholders' arrangements for procedures should specify the type or format of procedure (flowchart, tabular, check list, etc.) required for different types of activity that might be required in support of security.

30. Whilst the primary role of procedures is to support the conduct of operations ensuring consistent and high levels of human performance, procedures are

also an important component in the conduct or training and assurance of competence. Security role holders should demonstrate knowledge of and an ability to conduct tasks consistent with procedural requirements. It is important therefore that training is conducted using only approved procedures. This requires close cooperation between those with roles and responsibilities for procedures and training where these are held by separate role holders.

31. In conducting inspections in relation to this SyDP, inspectors should consider both the dutyholder's arrangements for the production and management of procedures and check the implementation of these by review of a sample of procedures of different types.

32. Inspectors should consider:

- Does the dutyholder have an adequate process for the production, maintenance, review, amendment and version control of procedures?
- Is there a process in place by which procedures are categorised for level of use and does this result in a useable set of procedures at the point of work?
- Can the dutyholder provide evidence to demonstrate high levels of procedure use and adherence? This may be in the form of performance indicators, results of event investigations or other metrics collected by the dutyholder.
- Does the dutyholder have processes in place to ensure technically correct and useable procedures are produced and an effective process for the amendment of procedures in response to user feedback? Inspectors may seek evidence of verification and validation exercises, data on procedure amendment numbers, time for amendment and extent of procedure amendment backlogs.
- Are the resources assigned to the production and management of procedures adequate? Consider both the number of personnel assigned to the role and their competence.
- Are the interfaces between different roles involved in the production and use of procedures adequately managed? This should include interfaces between roles involved in procedures, training and the production of security documentation such as the security plan and security risk assessments as a minimum.
- In their review of samples of procedures, inspectors should confirm that:
  - Content is clear and unambiguous.

- They clearly describe how tasks will be carried out and contain all necessary prerequisites, checks, precautions, and actions to be taken in the interests of nuclear security.
- The level of use of the procedure is clearly identified.
- The period for review and update is clearly identified in order that operators can confirm a procedure is in date.
- They are consistent with the directions contained within procedure writers' guides where these are used.
- Procedures provide information necessary to recover from equipment malfunctions, faults, or human failures during security operations.

- Where it is possible to undertake a site-based intervention related to procedures, inspectors should also seek evidence that:
  - Personnel have the necessary procedures at the work site and that they are being used appropriately during task completion.
  - Security/ operations / maintenance personnel understand the conditions for use and the meaning of the procedure, and whether they consider it provides a clear and adequate understanding of their task.
  - Personnel understand the dutyholder's expectations regarding procedure use and adherence.
  - Personnel understand what to do if they identify an error in the procedure or they do not fully understand its content.
  - Seek evidence from personnel that the procedure amendment process is effective and that changes to procedures are adequately tested and communicated.

8. Administrative Controls

33. Administrative controls are a subset of tasks important to nuclear security, being those human based processes that provide the delivery of security functions. These human based processes are the people and procedural components of the protective security arrangements. It is important that claims made on such administrative controls are substantiated in a dutyholder's security plan or supporting documentation.

34. Appropriate methods for the substantiation of administrative controls include the use of:

- Task Analysis.
- Allocation of Function.
- Human Failure Analysis.
- Assessment of Performance Influencing Factors.

35. The substantiation should demonstrate the tasks encompassed by the administrative control are feasible, that the potential for human failure has been reduced, and that human performance is supported by the design of workspaces, equipment and procedures. Advice on appropriate human factors methods for undertaking substantiation and the provision of evidence in relation to administrative controls is provided in CNS-TAST-GD 3.1 [8].

36. Inspectors should consider:

- Has the potential for error and violation and malicious acts during implementation of the administrative controls been identified and guarded against? (See [8])
- Does the design of working environments, equipment and interfaces support completion of the administrative control? (See [9])
- Are administrative controls adequately covered by the Dutyholder's training and competency assurance arrangements? (See [10])
- Are the requirements of administrative controls adequately presented to personnel in written procedures?
- Has the effective completion of administrative controls been demonstrated by processes of validation, exercise or operational experience review?

37. Administrative controls with an impact on nuclear security can extend beyond those directly identified for the delivery of security functions in the protective security arrangements. These include temporary security plans or arrangements that may be required to maintain legal compliance during

planned or unplanned engineered security system outages. Where such administrative controls are used, dutyholders should demonstrate the robustness and reliability of the control.

References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”.

[6] IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.

[7] IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011.

[8] ONR, “CNS-TAST-GD-3.1 Identification and Analysis of Security Tasks and Roles”.

[9] ONR, “CNS-TAST-GD-3.3 - Workspaces Equipment and User Interfaces”.

[10] ONR, “CNS-TAST-GD-3.2 - Sufficiency and Competence of Personnel Delivering Security”.

Glossary and Abbreviations

CCTV	Closed Circuit Television
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
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PPS	Physical Protection System
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide