Sufficiency and Competence of Personnel Delivering Security			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-3.2	**Issue No.:**	3
Record Reference:	2022/14794		
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') [1] may also use 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 analysis of competence, number and organisation of personnel required to deliver nuclear security. 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 3.2 – Sufficiency and Competence of Personnel Delivering Security, 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 ONR’s Classification Policy [4] describe 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. 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.

11. A more detailed description of the elements is provided in Recommendation's level guidance, specifically Nuclear Security Series (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.

12. The IAEA also publishes NSS 12 "Educational Programme in Nuclear Security" [8]. It is intended for a range of people with responsibility for nuclear security including university curriculum developers, nuclear security instructors and human resource development managers. The scope of this publication is broad and covers education in all areas of nuclear security, ranging from MSc programmes for developing highly educated staff with in-depth knowledge to a programme for the development of certified nuclear security specialists.

13. This TAG is also consistent with the Systematic Approach to Training, advocated by the IAEA in Technical Document 1254 [9] and implicit in other publications [10] and [11] .

5. Advice to Inspectors

14. Humans play a key role in the delivery of nuclear security, forming an integral part of the protective security arrangements and response to a nuclear security event. Effective human performance is dependent on a dutyholder having an adequate number of personnel and determining how best these can be organised to deliver the required security outcomes; this is termed the staffing design.

15. Competency management arrangements must also be in place that identify the required competencies of all personnel who contribute to the delivery of nuclear security. These arrangements should also provide for a systematic approach to nuclear security training which identifies training objectives and needs, provides well designed and delivered training and competency assessment materials, and evaluates and improves the training process. The competency management arrangements must be supported by an adequately resourced and managed training function.

16. This TAG informs regulatory assessment of the management of human performance and addresses the aspects of staffing design and competency management. It establishes ONR's expectations of the dutyholder's arrangements for these aspects. It provides guidance to inspectors on:

- Staffing Design
  - Staffing arrangements,
  - Team design,
  - Design of shift work systems,
  - Analysis of workload.
- Management of Competence
  - Analysis of roles and competencies,
  - Identification of learning objectives and training needs,
  - Design of training,
  - Assessment of competence,
  - Evaluation of training effectiveness
  - Organisation and support of the training function.

17. This assessment guide focuses on the analysis of staffing design and management of competence, presenting a summary of the reasons why it is an important component of a dutyholder's human performance management arrangement, and sets out the principal factors which should be considered by the ONR inspector. The guidance should be applied in a proportionate and targeted manner during assessment of security plans for all stages of operations. This includes the design and modification of new and existing facilities and justification of the adequacy of existing operations and decommissioning. In addition, such analysis should be applied where shortfalls in engineered controls are compensated for by procedural and

administrative controls either on a temporary or permanent basis (e.g., where an automated pass reader is replaced by a guard force pass check at an entry point to a site or facility).

18. The emphasis that the inspector gives to assessing different elements of a dutyholder's staffing design and competence management arrangements will depend upon the plan being assessed and application of the graded approach. For example, where the tasks involved in carrying out a role are already well-defined, it may not be necessary to closely scrutinise the processes used to analyse the staffing and competency management arrangements. Conversely, where new activities are being developed, or modifications being proposed, closer examination of the approach which the dutyholder takes to analysing these factors may be appropriate. As an overriding principle, the inspector should consider the security significance (the relevant outcome, security function category or the categorisation for theft or sabotage) of the activities concerned and adopt a proportionate and targeted approach to applying the guidance in this document.

6. Regulatory Expectation

19. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies how they adopt a systematic approach to identifying the numbers of staff and the staffing design required to deliver the defined security functions as well as a structured and systematic approach to the management of competence for all staff involved in the delivery of security.

FSyP 3 – Management of Human Performance	Sufficiency and Competence of Personnel Delivering Security	SyDP 3.2
Dutyholders should demonstrate by analysis that they understand the numbers and competencies of personnel required to deliver all security functions, and that they have a systematic approach to identification of their training needs and competence management.		

7. Staffing Design

7.1. Staffing Arrangements

20. In the context of this document, Staffing Arrangements refers to the arrangements to ensure an appropriate number of Suitably Qualified and Experienced Persons (SQEPs) are in place to control activities that could impact on nuclear security under all foreseeable circumstances throughout the life cycle of the process or facility. Ensuring that the appropriate number of competent people are organised and deployed in the right way is fundamental to nuclear security and safety. The Nuclear Baseline (NB) is a possible means by which the dutyholder may demonstrate that its organisational structure, staffing and competencies are, and remain, suitable and sufficient to manage nuclear security throughout the full range of its business (see CNS-TAST-GD-1.2 [12] for more guidance on the application of the nuclear baseline to security and [13] for more general guidance on the nuclear baseline.

21. The dutyholder's security plan should include a description, with rationale, of the staffing levels (numbers of personnel) that are required to carry out roles that have the potential to impact on nuclear security. NISR specifically requires that the manner in which the nuclear premises are to be policed and guarded, including the identity of the person providing any constables or persons acting as guards, the total number of constables and such persons attached to the premises and the number of such constables or other persons who will normally be present there. Staffing levels can be derived from an analytical process that makes use of task and workload analysis tools, (see CNS-TAST-GD-3.1 [14]) or be based on evidence gathered from operating experience, from predecessor facilities or from similar facilities. In some cases, a mixture of approaches may be used, with detailed analytical tools used to justify the staffing arrangements for those roles that have a high potential impact on nuclear security e.g., guard force personnel, security control room personnel, with fewer formal methods being used for those roles that have a less direct role in achieving nuclear security e.g., operating staff and managers.

22. The ONR inspector should confirm the dutyholder has a structured process in place to identify the responsibilities/tasks which are to be performed for each security important role, and the competencies needed to perform these tasks. The output of this process should contribute towards the specification of a role profile. An individual post may include a number of roles, and these should be set out in the job description. Where this is the case, consideration should also be given to the integration of these roles within a 'post' to ensure they are compatible and do not either overload individuals or create conflicts in terms of responsibility or delivery. The job description and role profile should explicitly include, or reference, the competencies needed to carry out the associated activities.

23. The analysis of staffing levels should include periods within each of the government response levels and security event conditions.
Staffing arrangements must recognise that staff numbers should provide sufficient resources to cover time needed for training and development of personnel and to cover for absences e.g., due to holidays and sickness.

24. The analysis of staffing levels should also take into account the number of staff required to support delivery of the security regime for example those involved in workforce trustworthiness and the provision of aftercare services.

25. Where nuclear security roles are provided by staff external to the dutyholder, the staffing arrangements should provide sufficient staff numbers to provide oversight and supervision of contract staff as well as the numbers of contract staff required to fulfil security roles.

26. Dutyholders should provide evidence to validate the adequacy of staffing levels outlined in their security plans. This evidence may be provided by operating experience reviews of security performance, security contingency exercises and site emergency exercises.

27. Benchmarking serves a useful purpose in enabling dutyholders to compare their approaches to staffing and task organisation to those of other organisations. This is particularly relevant for new nuclear facilities or those changing status, such as during commissioning or decommissioning. Therefore, the ONR inspector should review whether the dutyholder has compared their arrangements for staffing and task organisation against those of comparable facilities, and any impact of staff morale on security risks and culture is understood.

28. Inspectors should consider:

- Has the dutyholder carried out task and workload analysis where appropriate to determine the necessary staffing arrangements for nuclear security tasks and roles identified in the security plan?
- In cases where staffing levels are based on operating experience, predecessor or similar facilities, has the dutyholder systematically considered and addressed any differences that might impact on the appropriateness of the staffing arrangements?
- Do the dutyholder's staffing arrangements consider periods of normal operation, periods of heightened security threat levels, nuclear safety events, and requirements of the security contingency plan?
- If applicable, have the potential implications of sharing staff between multiple areas, facilities or sites been considered including cases where personnel may be co-opted from a shared pool?

- How has time for training and personnel development as well as the impact of leave and sickness absence been factored into the determination of staffing levels?
- Does evidence from safety and security exercises support claims that staffing arrangements are adequate to respond to challenging and resource intensive scenarios?
- Is there evidence of effective management of staffing levels above the required minimum, for example rapid call-out due to unexpected absence?
- Do qualitative and quantitative indicators support claims regarding adequacy of staffing levels? Indicators of potential problems include:
  - High levels of overtime.
  - Symptoms of personnel stress due to under or overload (high levels of sick absence, high employee turnover, high numbers of grievances).
  - High levels of maintenance or procedure update backlogs.
  - Deferral or delay to nuclear security improvement programmes.
  - Event investigations identifying staffing issues as root causes.

7.2. Team Design

29. Inadequacies in team design have been implicated in major events in the nuclear and other industries. Key factors which contribute to effective team design include team size and composition, clarity of roles and responsibilities, communication and supervision, including spans of control, (i.e., the number of sub-ordinates that can be effectively managed by a supervisor or manager). There are differing views on what constitutes an optimal span of control (ranging from 5 to 20 people). There are advantages and disadvantages to both wide and narrow spans of control. Narrow spans of control are usually more hierarchical and have more reporting layers. Supervisors may therefore be able to spend more time with staff, but conversely, communication difficulties can occur if there are a large number of reporting layers. Wide spans of control may create a flatter, more flexible organisation but may also result in supervisors being overloaded. The dutyholder should demonstrate that they have considered these factors as well as the level of competency of the supervisor and team members, culture (for example the degree of alignment of goals), and task characteristics.

30. Inspectors should consider:

- Does the composition of teams involved in nuclear security related work include the necessary mix of skills, in sufficient numbers to effectively carry out the functions and tasks required of them? Inspectors should consider both front line functions such as access control, perimeter

monitoring, threat detection and support functions whose actions impact on these e.g., maintenance or communications.

- Has the dutyholder established appropriate spans of control?
- Have supervisory requirements for security claims on control room and field teams been systematically identified?
- Are the following clearly defined for different operating conditions where applicable?
  - Roles, responsibilities and accountabilities within teams.
  - Interfaces between teams, including contractors where applicable.
  - Interfaces between CGF, CNC and Home Office Police where applicable.
- Are there effective formal and informal mechanisms in place for communication between teams? e.g., central control teams, field teams and those external to site, respective shifts, dutyholder and contractor organisations.

7.3. Design of Shift Work Systems

31. The design of shift systems is an important part of staffing design that impacts on human performance. The type and nature of the shift system design can impact both positively and negatively on worker health and wellbeing which in turn impacts performance. Poorly designed shift systems can increase fatigue which is generally considered to be a decline in mental and/or physical performance that results from prolonged exertion, sleep loss and/or disruption of the internal clock. Fatigue makes it harder to concentrate, reduces vigilance and situational awareness, impairs decision making, reduces motivation or interest in work and can slow reaction time.

32. Where dutyholders propose changes to shift patterns or durations, ONR expects that this is managed via a systematic process such as Management of Change. These should include features such as staff involvement and consultation, pilot testing prior to full implementation, review of lessons learned from similar changes in the same or equivalent organisations and the tracking of the impact of the change by measurement of Key Performance Indicators.

33. The HSE provides advice on good practices with respect to the design of shift schedules (see [15] and [16]). This identifies a number of factors that reduce fatigue including:

- forward rotation (mornings/afternoons/nights),
- very fast (2-3 days) or very slow rotation (3-4 week) rotation.

- Adequate rest and recovery periods between individual shifts and series of consecutive shifts.
- Avoidance of early start times (before 0700)
- Shift length and type of work, short shift lengths (i.e., eight hours) better for work that is complex, monotonous, requires vigilance or is machine paced.

34. Inspectors should consider:

- Has the dutyholder carried out an assessment of proposed or existing shift schedules using an appropriate tool such as the HSE fatigue/risk index?
- Does the proposed or existing shift system adopt the good practices for shift design identified in HSE guidance?
- Does the dutyholder have management arrangements in place to monitor and control hours worked including overtime?
- Does the dutyholder's management arrangement for control of hours worked control shift swapping and second jobs?
- Does the dutyholder have a process for managing resource shortfalls, does this include identification and implementation of suitable compensatory measures?
- Are adequate arrangements in place to plan, control and implement changes to shift schedules?

8. Workload

35. Workload is a key performance influencing factor that impacts on the quality of human performance. Workload can be measured in a number of ways all of which relate to the amount of demand that a task or series of tasks place on individual personnel or teams of people. Workload can be assessed in terms of the:

    - Physical demand made on a person in terms of the amount of the intensity of physical activity and duration for which it needs to be delivered.
    - Cognitive demand in terms of the amount and intensity of mental processing needed to complete a task, including demands on attention, perception, memory and decision making.
    - Time demand in terms of the amount of time that a person is engaged in mental or physical activity relayed to the total time available to them in a shift.
    - Supervision demand in terms of the span of control or the number of personnel each supervisor is responsible for and the number of supervisory tasks and amount of direct supervision that need to be provided.

36. Analysis of workload is important for the demonstration that tasks allocated to humans are within their capabilities i.e., in support of SyDP 3.1 and for the demonstration that a dutyholder has an appropriate number of competent staff available to complete all tasks important to security (this SyDP).

37. Analysis of workload is important because excessive workload can increase the likelihood of human failure and degrade other aspects of task performance such as speed and quality of performance. Too little workload can also have negative effects on performance such as reduced vigilance, situational awareness and an increased likelihood of violation resulting from boredom. Unbalanced workloads can result in reductions of job satisfaction leading to low motivation and high staff turnover. Workload assessment is necessary to show that demand during periods of normal operation is not too high or too low and also to demonstrate that sufficient capacity is available to cope during periods of increased demand e.g., during security events.

38. Workload analysis should be performed when new tasks are added to a role, both to demonstrate that the task is achievable and also to measure the impact on overall workload. Similarly, the workload associated with the introduction of new equipment or new team or shift structures should be assessed in order to demonstrate that any impacts on human performance are positive or neutral.

39. Workload analysis can be undertaken using a range of analysis techniques which typically involve talking to or using questionnaires with those who complete the tasks. Data on workload can also be gained both by observing security exercises and seeking feedback from participants after the exercise is completed. Inspectors should expect that some consideration and assessment of workload is included as part of the evaluation of exercises and events should they occur.

40. Inspectors should consider:

- Has the dutyholder undertaken an assessment of workload for key roles involved in the delivery of security functions?
- Does the dutyholder's approach for the assessment of workload use recognised methods of workload assessment?
- Is the dutyholder's assessment of workload supported by evidence gained from exercises or reviews of security events?

9. Competency Management

41. It is essential that personnel whose activities have the potential to impact on nuclear security are Suitably Qualified and Experienced (SQEP) to carry out their jobs. This includes those who directly carry out security operations and others such as directors, managers, internal assurance, designers, security plan authors, Occupational Health practitioners, (etc) whose roles, if inadequately conceived or executed, may affect security in less visible ways. For example, through introducing latent technical or organisational vulnerabilities. Dutyholders should, therefore, put in place robust arrangements for identifying its competence needs and assuring these are met and maintained. The arrangements should clearly define the dutyholder's interpretation of SQEP and should identify those who need to be SQEP. Staff who discharge nuclear security roles should be included within the dutyholder's organisational baseline (see NS-TAST-GD-065 [13]).

42. Security Delivery Principle 3.2 in SyAPs confirms there may be a need for the appointment of Duly Authorised Persons for Security Purposes (DAPSyPs). DAPSyPs are usually identified as individuals who are in direct control or supervision of operations or activities that impact on the security regime of a site or facility, notwithstanding the role may not necessarily be their primary function. Their appointments are therefore subject to additional management controls covering areas such as appointment and assessment. Roles for which DAPSyPs need to be appointed should be specified in the dutyholder's security plan, and a register kept of such persons. However, the general principle is that persons whose activities may impact upon nuclear security should be appropriately trained, and their competence adequately assured, is similar for SQEP personnel and those designated as DAPSyPs

43. IAEA has defined competence as "the ability to put skills and knowledge into practice in order to perform a job in an effective and efficient manner to an established standard" [11]. ONR concurs with this definition, which is widely accepted within the international nuclear community. Training is a fundamental mechanism through which personnel acquire, and maintain, the skills and knowledge needed to perform a job to defined standards. Other factors contributing to a person's competence include their prior experience, aptitude, attitude, behaviours, skills and qualifications. Competence can therefore broadly be equated to SQEP.

44. ONR considers that training should be instrumental in developing and sustaining competence. This training may build on and contextualise competencies developed by achievement of a formal qualification and/or experience gained elsewhere. In some cases, dutyholders may claim that qualifications and/or prior experience means that additional training is not required to develop specific competencies. In such cases, the inspector should consider how the understanding of local context and specific aspects of the dutyholder's arrangements in which these competencies are applied is developed and assured in individuals. Dutyholders should also have

arrangements in place to define and deliver the training needed to sustain competence, and these arrangements should be clearly detailed in their security plan.

45. The dutyholder should have a process in place to ensure that security roles performed by staff whom it does not employ directly (e.g., contractors such as guard force/security system engineers and agency staff) have been suitably identified and are subject to the dutyholder's arrangements.
The responsibilities/tasks associated with each role then need to be determined so that competence and training needs can be assessed and established, and judgements of competency be made. Where training and competency assurance for security roles is provided by those supplying external staff, this should be supplemented by dutyholders to ensure that contractors understand the site topography, operations, hazards and associated controls and expected behaviours.

46. A well-designed training and competence management system should adequately address the following elements, and these are likely to be areas of focus for the inspector:

- analysis of roles and associated competencies,
- identification of learning objectives and training needs,
- training programme design,
- selection of appropriate training methods and media,
- assessment of competence,
- evaluation of training effectiveness,
- organisation and support of the training function.

47. These elements should not be considered as independent of one another or standalone activities. Rather, it is expected that a dutyholder's competence management system should reflect a systematic approach to training encompassing the analysis of competencies and identification of training needs and development of training programmes which are systematically reviewed and updated in response to learning from experience, benchmarking from other dutyholders and from self-evaluation processes.

9.1. Analysis of Roles and Competencies

48. The starting point for the development of a competency management system, is an understanding of the set of competencies required to deliver each of the roles necessary for security. Identifying the components of a role, and the competencies needed to carry them out, is likely to involve the use of job/task and competency analysis. Whilst job analysis involves identifying the tasks associated with a role, task analysis involves obtaining a more fine-grained

understanding of how a task is performed. Both job and task analysis can be used for the identification of the competencies associated with a role. Where tasks are relatively simple a task listing may be sufficient to identify required competencies. Where tasks are more complex a breakdown of the overall task into its constituent parts may be required.

49. A range of task analysis techniques is available to dutyholders, and the choice of technique should depend on the nature of the activity and the information being sought. Useful guidance on the selection and use of task analysis techniques is provided in the CNS-TAST-GD 3.1 [14]. Job and task analysis can be a resource-intensive activity, and it should not be necessary for a detailed analysis to be performed for every role. Factors that determine the use of job and task analysis methods include the difficulty or complexity of tasks, the importance of the task for the achievement of security outcomes and the frequency with which tasks are performed. Consideration of these factors is often referred to as DIF (Difficulty/Importance/Frequency) analysis when a systematic approach to training is applied.

50. For each role and associated task(s), both the competencies needed to carry out the work, and the level or standard which those competencies must meet, should be determined and documented. The set of competencies should include both technical elements and others which may be less tangible, but which are no less important, such as decision making, challenge, management and leadership, communication and behavioural skills, etc. The competence requirements for all nuclear security roles are expected to include an awareness of the importance of sustaining and contributing to a strong security culture and the importance of attitudes and behaviours in relation to this. All staff should understand why nuclear security is important and that their roles and responsibilities require working in a way that promotes safety and security. The systematic approach to training typically identifies competencies in terms of:

- Knowledge, what the person needs to know and understand,
- Skills, what the person needs to be able to do,
- Attitudes, the way in which a person approaches their role in terms of the value they place on achieving security and the diligence with which they apply their knowledge and skills. Individual attitudes to security are likely to be shaped by the culture within an organisation as well as broader societal norms.

51. Dutyholders should ensure that where nuclear security is dependent on those who operate predominantly in an operational role, conflicts between safety and security requirements are quickly identified and resolved after due consideration and balancing of the relative risks.

52. In addition to consideration of individual roles and tasks, analysis should include consideration of the way in which these come together and how team and organisational performance can impact upon security. This should input to

and be reflected in the process for identifying the required competencies, in terms of knowledge of people's roles and interactions between those who make up the security system, skills that underpin teamworking such as communication and supervision as well as attitudes to others and the importance of teamworking.

53. When considering the range of competencies that are needed to fulfil a designated role, the dutyholder should consider circumstances where an individual may be called upon to deputise for another person (e.g., sickness or holidays). Although the deputy may not possess the full range of competencies required to carry out the work on a long-term basis, the dutyholder should identify the principal security-related activities and ensure that the Deputy is, and remains, competent to carry out them out for the necessary periods of time.

54. Inspectors should consider:

- Has a suitable analysis been carried out to identify those roles that may impact on security, including corporate as well as security operations staff?
- Is the analysis sufficiently detailed to provide confidence that all security-related roles and responsibilities have been identified?
- Does the analysis include consideration of the full range of operating states, including during periods on increased alert or response level and when security events identified in the security plan occur?
- Is the analysis current (i.e., has it been maintained to take account of plant, equipment, procedural or organisational changes)?
- Have the competencies required to carry out the tasks or activities associated with each role in an efficient and effective manner to the designated standards been formally identified?
- Has the identified set of skills, knowledge and competencies been used to inform the selection criteria for specific roles and posts?
- Do the identified competencies include managerial, leadership and behavioural factors?
- Has consideration been given to the competencies required to support team and organisational performance as well as for individual roles?
- Have any DAPSyP roles been identified and are their associated competencies clearly defined?

9.2. Identification of Learning Objectives and Training Needs

55. The analysis of roles, tasks and competencies should be used as a basis from which to identify learning objectives and training needs. A training need is identified where analysis or data demonstrates that a required competence or set of competencies is not found in current role holders or is unlikely to be found in new appointees to a role. Training needs may also arise as a result of the introduction of new work processes, equipment or regulatory requirements that introduce new competencies or change the existing competencies required for a specific role.

56. A learning objective is a statement of the skills, knowledge and attitudes that a role holder or trainee will be required to transfer to a responsibility/ task to a defined performance standard. For example:

- A security control room operator will be able to carry out an immediate assessment of a perimeter alarm utilising the CCTV system whilst co-ordinating activities with colleagues where appropriate to achieve the required outcome.
- An investigator will be able to undertake a suitable event analysis, using appropriate techniques and procedures, identifying appropriate causes for an event.

57. These learning objectives should inform the development of a set of training outcomes, and should be used to derive the criteria, or standards, against which a role holder or new appointee is assessed before, during and/or after training.

58. Although dutyholders may choose to put their staff through training programmes which cover all the learning objectives identified in this way, this may not be essential. Each person will bring certain skills and experience to their job and a review of these, and application of appropriate selection techniques, may remove or reduce the need for training to be provided for every facet of a job and identified learning objective. Thus, it is reasonable for the dutyholder to consider the competencies which a person already has by conducting a gap analysis and target its training effort on those objectives where the person is not demonstrably competent. Nonetheless, in circumstances where learning objectives are deemed to be met on the basis of existing qualifications or experience, the dutyholder should satisfy themselves and record evidence of the basis for this decision.

59. Although it is important that the dutyholder's approach to staff selection is rigorous and effective (see [11]), ONR places emphasis on the adequacy of the dutyholder's training arrangements and, in particular, the measures used to determine, monitor and sustain competence. Regardless of the previous experience and qualifications of the candidate, the dutyholder should ensure that the competencies needed of each role and post-holder have been

identified systematically, and that training is provided for all those areas in which the person is not able to demonstrate an adequate level of competence. As noted above, these should include all aspects of competence including knowledge, skills and attitudes.

60. Inspectors should consider:

- Has the dutyholder used a systematic approach incorporating job, task or competency analysis to identify a set of learning objectives associated with each role necessary for the delivery of nuclear security.
- Have the identified learning objectives been distilled into an outline set of training needs?
- Does the set of training needs take account of the required qualifications, skills and experience of the role holder and the need for these to be refreshed?
- Have the standards which should be achieved in order for a person to be considered competent been defined?

9.3. Design of Training

61. Inspectors should consider design of training at two levels, the design of the overall training programme which should address the totality of the competencies needed for a particular security role, and the design of individual training methods and media which can be considered at the level of individual elements of training. It is possible that a dutyholder could design an appropriate training programme but that this could fail to deliver the required competencies because of poorly selected training methods and poorly designed training materials. Conversely, a dutyholder may have examples of well-designed training material, delivered using appropriate methods, but the range of material may not address all of the learning outcomes or focus too heavily on outcomes that make a minor contribution to nuclear security.

62. A training programme should be designed by a SQEP individual to help develop and maintain the competence of all personnel with security responsibilities. The starting point for the training programme should be the competence requirements and learning objectives of the role-holder and their competence gaps as identified through a gap analysis. The training programme should specify how those objectives are to be achieved.
The training programme can be viewed as gathering the different elements into a focused and coordinated schedule to support the development of competence for a given role. The training programme for each role should identify what learning objectives must be met by **initial training** and which of the objectives will need to be refreshed or extended at prescribed intervals by **continuation training**.

63. It should be recognised that there is a need to encourage a positive security culture in all staff, and training programmes should seek to build in and promote an awareness of security culture and its attributes. It is important that all personnel, from the board down, receive training which supports the security culture of the organisation, through developing the right attitude to security by informing personnel about the behaviours, expectations and management arrangements that help ensure an effective approach to nuclear security. Such security attitudinal training aimed at a wide audience may be achieved by a variety of means such as by making use of the dutyholder's established communication channels/methods for imparting key messages, for example providing ongoing communications to staff about issues such as phishing emails. The need for training to reinforce an appropriate security culture, as well as enabling the acquisition of technical competence, is acknowledged by IAEA. Such training should encompass lessons learned from case histories of security events (e.g., Y12), and the underlying organisational and cultural factors that impacted on them. Contractors should be included in such training.

64. **Initial training** programmes should cover all the training needed to enable personnel to work in specified roles and posts. This should include basic induction training which applies to all personnel and covers items such as security hazards and risks and their control measures, secure working practices, actions to take in response to security events etc, as well as job-specific training. In addition to the outputs of the role and task analysis, security plans should be used to identify activities which warrant particular attention during training. For example, tasks upon which significant nuclear security claims are made should be highlighted in training and should be extensively exercised to ensure they are properly and consistently undertaken, particularly where these are skill based or form part of an emergency response. Tasks which are complex, or which are performed infrequently, and hence irregularly practiced, may need identifying and warrant special attention. In the case of infrequent tasks, consideration should be given to the timing of training and its delivery, so it is provided in good time but not so far in advance of when it is needed that it is forgotten.

65. **Continuation training** should also be programmed to help maintain competence, especially for tasks associated with roles which are security-significant and those which are complex or infrequently performed (e.g., by those deputising for others). Different groups may have differing continuing training needs. For example, security operations staff should have the opportunity to rehearse knowledge of the security plan (including security contingency arrangements) and operating rules, and to engage in team training. Maintenance personnel, and those supervising or approving maintenance activity, may require training in the use of equipment needed during infrequently performed activities and in the relevance of their work to the security plan. Supervisors and managers should receive training in security management, leadership, communication, and other supervisory skills. Training should be used to update personnel on operational experience feedback and the implications of modifications to plant, operating regime and

instructions as well as personal development needs. Work to reinforce a positive security culture should be a consistent feature of continuing training.

66. Training of staff involved in dealing with security events is an important aspect of continuing training. Training should address a comprehensive range of scenarios, both to support the development of personnel competence, and to improve the site and/or facility's emergency preparedness and response arrangements. This should include consideration of a full range of competencies such as leadership, command and control, teamworking, interpersonal communications, stress resilience and decision making.

67. The training media and methods which are used to develop the competencies required in different roles should be both effective and practicable. This demands that careful attention is given to the choice of training media and to the way in which those training media are then used (i.e., the training method). The dutyholder should, therefore, be able to show that it has considered and identified appropriate media and methods to support the training for different tasks.

68. A range of different training media and methods are available, including the following principal examples:

- **Classroom teaching** may be most suitable for introductory material and where detailed information of a theoretical or conceptual nature needs to be learnt. This medium also allows tasks to be talked or walked through, this can include the conduct of tabletop security exercises to rehearse how security threats may be dealt with. However, classroom teaching allows the trainee limited opportunity to gain hands-on experience in performing a practical task, or to put conceptual learning into practice.

- **On-job training** is an essential part of most training programmes and provides a realistic environment for the trainee. However, it can be difficult to ensure systematic and controlled on-job training because the learning environment may be less easily controlled. In addition, concerns about the potential impact of trainee error on security-significant tasks may limit the suitability of this approach for some activities. The dutyholder should be able to demonstrate that on-job training is properly specified, provided by people suitably SQEP (i.e., competent) to carry out that function, and that adequate control and supervision is in place.

- **Simulation** allows the rehearsal of practical skills under controlled conditions. Simulated safety and security exercises and the use of replica equipment can be used to train groups of security and other staff, although it is noted that this is resource intensive. Whilst it is unlikely that dutyholders will have security control room simulators, there may be secondary security control rooms that could be utilised for training specific actions such as response to security events and

alarms. Low fidelity task simulation (e.g., tabletop exercises) may also be used.

- **Open learning techniques**, in which training is provided through structured self-teaching packages, are increasingly popular owing to their flexibility and cost-effectiveness. These techniques may employ advanced technology such as computer or tablet-based packages and interactive video as well as more conventional methods. Care should be taken to ensure that open learning is fit for purpose, and that it is not used at the expense of other forms of training without justification and demonstrable benefits.

- **Briefings** which may not be formally structured in the same way as other training approaches, can play an important role in training. These will typically involve discussions, often led by a manager or team leader, on factors affecting the way in which jobs are carried out, for example, adherence to procedures, security culture, communications etc. It should be noted that such briefings tend to be more effective when they are formally structured, require active participation and check that their content is understood by the attendees.

69. Delivery of training requires instructors who have the appropriate knowledge, skills and attitudes for their area(s) of responsibility. They should thoroughly understand all aspects of the security training syllabus they are responsible for delivering, and the relationship between the course content and security operations. Additionally, the instructors should be familiar with the basics of adult learning and a systematic approach to training and should have adequate instructional and assessment skills.

70. The inspector should confirm the dutyholder has considered the choice of training methods, and the way in which these are used, as well as the training materials that support them. The dutyholder should be able to demonstrate that the selected training methods and materials promote effective development of the learning objectives and competencies which have previously been specified.

71. Inspectors should consider:

- Has the dutyholder established an initial training programme for all personnel whose duties might impact upon security, including the board, managers and contractors, as well as other staff?

- Does the initial training programme include induction training to ensure a basic understanding of the employee's responsibilities, secure working practices, generic security-related matters and the threat?

- Does the training programme identify activities which are security-significant, complex or infrequent and which warrant particular attention during training?

- Does the training programme recognise the need to address leadership, managerial, behavioural, communication and security culture issues as well as individual competence?
- Has the dutyholder established a continuation training programme for all personnel whose activities at work might impact upon security?
- Does the continuation training programme clearly define and justify the training schedule and periodicity for different activities?
- Does the training programme identify when training is needed, and how it should be delivered, assessed and evaluated?
- Are the dutyholder's chosen training media and training methods based upon a consideration of how best to achieve the learning objectives?
- Are simulated exercise material and other training equipment kept up to date such that they reflect changes to the site and its security equipment and arrangements?

9.4. Assessment of Competence

72. Each person who carries out activities which may affect the security of a nuclear facility or site should be demonstrably competent to perform their security role. Although training plays an important role in developing the necessary competencies, it does not itself guarantee competence: if training is poorly specified or targeted, or the trainee is not suited to the job, then a person may fail to achieve an acceptable level of performance.

73. For these reasons, ONR regards the assessment of a trainee's competence and, subsequently, the periodic re-assessment of personnel, as a key element in the process of developing and maintaining the competencies needed to function as a SQEP or a DAPSyP. When properly defined and carried out, assessment serves the following important functions:

- Demonstrating that learning objectives have been achieved and a level of competence attained
- Identifying the need for refresher or additional training through identifying shortfalls in performance
- Indicating whether training has been effective in developing the required competencies. In particular, assessment can point to deficiencies in identifying training needs or the design and delivery of training programmes.

74. Dutyholders should, therefore, satisfy themselves that all staff and contractors whose actions have the potential to impact upon nuclear security meet their competence criteria. When an individual is first appointed to a role, they may not be fully competent to carry out all the duties expected of them. Thus, the

competence assessment process should be used to inform a management decision to restrict the individual's range of tasks or decisions to those for which they are competent (e.g., a member of the guard force may be competent to detect security threats at the site perimeter but may not be confirmed as SQEP to do so in a site security control room using remote monitoring equipment). More generally, training records and assessments of competence should be actively used by Dutyholders when making operational decisions on deployment. Thus, they should be seen as a management tool. Not simply a process by which compliance with SQEP requirements is demonstrated. A dutyholder's management team should positively encourage staff and contractors to raise any concerns about their own competence or readiness to carry out a task and to seek further training or advice as necessary.

75. Dutyholders may use a range of different assessment methods. Their suitability will depend upon the training method and the nature of the competency being assessed. Traditional assessment methods that use paper-based question and answers may be appropriate for some activities but will be quite inappropriate for many others. For example, they might be a sound means of assessing an understanding of prohibited items but would not necessarily give an accurate indication of an individual's practical competence to undertake effective searching to prevent the introduction of prohibited items onto site or into sensitive areas. Assessment may take place on-the-job, within a controlled training/assessment environment, or in a workshop or a classroom. It may take place as a specific, defined activity or through continual assessment during training or performance in role.

76. In some circumstances, the dutyholder may wish formally to waive some parts of training. Such waivers should be kept to a minimum, but where training is waived, the dutyholder should still assess the affected person(s) to the same, or an equivalent, standard. This provides a basis for confirming that the person is competent, despite their not receiving the waived part of training. Where a contractor takes credit for prior training and the associated competences, the dutyholder should be able to show how it has satisfied itself that the contractor's training and competence assurance arrangements are adequate and confirm that they meet the dutyholder's expectations.

77. Regardless of the assessment method used, the dutyholder should be able to demonstrate that it is:

- **Valid** - i.e., it provides a reasonable indication of a person's likely performance on the real job. The criteria used to judge performance should therefore remain under constant review by the dutyholder.
- **Objective** - i.e., the less judgmental the assessment method and the criteria used to judge performance are, the less uncertainty there will be about the validity of the assessment. This is of particular relevance to on-job assessment.

- **Reliable** - i.e., if repeated, the assessment would be likely to produce consistent results.

78. Assessment should not be regarded as a one-off activity that takes place after initial training, and then 'qualifies' a person for the period that they subsequently remain in post. A person's competence may change over time as a result of influences such as the frequency with which a task is performed, the varying circumstances under which the task may be performed, or changes to plant or equipment. Loss of memory for the task and the procedures or arrangements which affect how it is performed may also be compounded by factors such as the development of bad habits, short-cuts etc. Changes to security system parameters or procedures may also take place when a person is away for an extended period and so affect their performance when they return to duty in a particular role. All these factors support the case for periodic re-assessment to ensure that personnel know about relevant changes to their working environment, and that they remain competent to carry out their jobs.

79. The frequency of re-assessment should be influenced by consideration of the following factors:

- The security significance of the roles and associated tasks which the person performs, as identified through the job and task analysis.
- The frequency with which the tasks are performed.
- Upgrades to the security technology necessitating new competencies.
- Operational experience feedback originating both within the dutyholder and from other organisations.
- Compliance with national standards or by those of accredited or authoritative bodies.

80. Inspectors should consider:

- Does the dutyholder have formally defined provisions for assessing the competencies of all personnel whose activities impact upon security?
- Has the dutyholder put in place robust processes to confirm its contractors are competent where they are not subject to the dutyholder's own competence assessments?
- Does the choice of assessment method reflect the nature of the competencies which are being assessed, and the training methods and media which are used?
- Can the dutyholder demonstrate that their assessment methods provide a valid, objective and reliable basis for determining competence?

- Has the dutyholder defined the periodicity of re-assessment which is appropriate for each job or task?
- Does the dutyholder act, in a timely manner, upon deficiencies in performance identified through the assessment or during training?
- Does the dutyholder have a defined strategy for addressing failures to meet the required standards following training?

9.5. Evaluation of Training Effectiveness

81. The effectiveness of training can be evaluated in a number of ways. At a most basic level training can be assessed on the numbers of people who successfully achieve the assessment criteria used to evaluate trainees' performance. Feedback on the training process by trainees and instructors can also provide insights to the effectiveness of training and provide data from which improvements to the training programme, delivery or assessment can be based.

82. Fundamentally, however, training is effective only in as much as the learning acquired through training transfers into the real situation. For example, security control centre training is of limited benefit if it provides trainees with the skills needed to operate individual equipment in the control centre, but not with the ability to operate different systems, possibly concurrently, to ensure timely identification of a threat and application of appropriate measures to meet the required security outcome. Similarly, classroom training which enables students to understand the effects of blast is, in itself, insufficient to develop operational competence in responding to suspicious packages. Dutyholders should therefore have a well-defined system for monitoring the effectiveness of training, and for identifying areas where training may need to be augmented or revised.

83. Evaluation of training effectiveness involves an intelligence gathering exercise, the purpose of which is to provide confidence that training has been specified properly, and that it is comprehensive, effective and up to date. As such, it should draw on a range of sources such as:

- Summaries of assessments of trainees, including trainee feedback.
- Self-assessments conducted by the training function.
- Operational experience feedback from the workplace including the results of event investigations.
- Security reviews and inspections conducted by internal and external assessors.

84. Inspectors should be satisfied that the dutyholder is 'closing the loop' by monitoring the systems which have been put in place to evaluate the effectiveness of each element of training. Where shortfalls in training are

identified (for example, via event investigations), dutyholders should demonstrate how the identified shortfalls in training have been addressed as well as how the training system itself has been strengthened.

85. Inspectors should consider:

- Does the dutyholder have in place a formal process to evaluate the effectiveness of training?
- Does the evaluation process use a suitable range of sources of information to judge effectiveness?
- Is the way in which training is specified, delivered and assessed monitored regularly?
- Do the findings of the evaluation process demonstrably influence the specification or implementation of the training arrangements?

9.6. Organisation and Support of the Training Function

86. The training and competence assurance of personnel with nuclear security roles should be regarded as a priority by dutyholders. ONR expects the dutyholder to show that the competence delivery functions are supported by a commitment to it from senior levels in the organisation and by an appropriate management structure. The commitment to competence and training should be embodied in a policy which recognises the need to develop and maintain the competence of staff in order to achieve and maintain nuclear security. It should also affirm the dutyholder's commitment to resource and maintain a training system and strategy that support implementation of the policy, recognising the need to accommodate a diverse range of staff and contractors who may have differing development requirements.

87. Organisation of the training function may differ from dutyholder to dutyholder, and it is not ONR's role to prescribe or define how this is done. However, responsibilities for training should be clearly defined, and the dutyholder should be able to demonstrate that training is being effectively resourced, specified, delivered, assessed, monitored and reviewed. This includes ensuring that training, which is provided by third parties, either on or off-site, is suitably specified and delivered. There should be a clear reporting route for departments or role-holders charged with responsibility for training which ensures that training issues can be raised at board level if necessary.

88. Where a training department is established, the dutyholder should ensure that adequate interfaces exist between training and other departments to identify training needs and make personnel available. The training department should be actively involved in helping line management organise training programmes for their staff and monitoring that line management implements these programmes. The training department may also take an active role in delivering certain elements of training.

89. The provision of effective training requires that personnel with a training role are themselves suitably qualified and experienced to be effective. It is important, therefore, that resources are made available for trainers to maintain and develop their own capability. Where training has been arranged so that it is delivered by a non-specialist (e.g., by an experienced person in the context of on-job training), the dutyholder should ensure the trainer is suitably equipped to carry out this role.

90. In recent years, dutyholders have placed increasing emphasis on the use of contract resource. Placing work with external contractors or agency staff does not negate or mitigate the dutyholder's responsibility for ensuring that all personnel whose actions have the potential to affect security are suitably qualified and experienced. External contractors may have been trained and assessed to different standards from those of the dutyholder's directly employed workforce. The dutyholder should have adequate arrangements to ensure that contractors are competent to work securely and efficiently and that the standards required of the contractors are consistent with those it would require of its employees. These should cover both technical competencies and also the other competencies and knowledge which contribute towards secure operations of a facility and the site (e.g., site induction training, communication skills, administrative arrangements and procedures, behaviours, etc.). The dutyholder should, therefore, put contractors through its own training and competence assessment programme, or otherwise satisfy itself that the contractor's own arrangements for ensuring the technical and behavioural competence of its staff are adequate.

91. ONR regards the design, control and maintenance of accurate training and competence records as essential elements for a dutyholder's approach to competence management. Such records enable training to be scheduled and delivered against a controlled statement of training needs. As such, they are a vital input to the planning process for training. They also provide evidence for both the dutyholder and ONR to ensure that training has been given and the competence of all personnel with security roles has been formally assessed.

92. The value of training records is related to the quality of information which is entered into them, and the use that is made of this information. The dutyholder should ensure that this information, and the design of the record system, enables training to be planned, scheduled, delivered and monitored effectively. Accordingly, training records should be subject to suitable quality management processes.

93. Inspectors should consider:

- Does the dutyholder have a training policy which sets out the company's commitment to training?
- Does the dutyholder have a management system for training personnel whose actions may impact upon security?

- Is the training function adequately resourced, in terms of staff numbers and capabilities?
- Are personnel who conduct training provided with instructional skills and guidance so that they can perform their roles effectively?
- If contractors are not subject to the dutyholder's own training and assessment practices, do the dutyholders ensure that the contractor's own arrangements for maintaining and demonstrating the competence of its staff are adequate?
- Are training records available and up to date, and are they controlled in an appropriate manner?
- Are the training records reviewed periodically so as to identify training or competence shortfalls or omissions?

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] IAEA, “IAEA Nuclear Security Series No. 12. Educational Programme in Nuclear Security”.

[9] IAEA, “TECDOC-1254 - Training the Staff of the Regulatory body for Nuclear Facilities”.

[10] IAEA, “Safety Report No.79. Managing the Regulatory Bodies Competence”.

[11] IAEA, “Safety Standard Series NS-G-2.8. Recruitment, Qualification and Training or Personnel for Nuclear Power Plants”.

[12] ONR, “CNS-TAST-GD-1.2: Organisational Security Capability”.

[13] ONR, “NS-TAST-GD-065 - Function and Content of the Nuclear Baseline”.

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

[15] HSE, “Research Report 446: The Development of a fatigue/risk index for shiftworkers,” 2006.

[16] HSE, “HSG 256 - Managing Shiftwork”.

Glossary and Abbreviations

CCTV	Closed Circuit Television
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
DAPSyP	Duly Authorised Person for Security Purposes
DIF	Difficulty, Importance, Frequency
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NB	Nuclear Baseline
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
PID	Passive Intruder Detection
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