Vulnerability Assessments			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-6.4	**Issue No.:**	1.1
Record Reference:	2022/20842		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Principal Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	Minor review to update references, comply with ONR style and accessibility guidance		

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 the exercise of their regulatory judgement during intervention activities relating to assessment of a dutyholder's processes for conducting vulnerability assessments of their site and facilities. It aims to provide general advice and guidance to ONR inspectors on how dutyholders' vulnerability assessments should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate.

4. A performance based vulnerability assessment should be carried out at all sites against the security outcome required from the physical protection system (PPS).

3. Relationship to Relevant UK Legislation and Policy

5. 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.

6. 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.

7. 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 6.4 – Vulnerability Assessments, in support of FSyP 6 – Physical Protection Systems. The TAG is consistent with other TAGs and associated guidance and policy documentation.

8. 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.

9. 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

10. 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.

11. Fundamental Principle J of the CPPNM refers to quality assurance and states that a quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. The importance of issues relating to quality assurance is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:

  e) Routinely conducting maintenance, training and evaluation to ensure the effectiveness of the nuclear security systems;

  h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

12. A more detailed description of the quality assurance is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [7]. This document states “A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.” NSS 13, Para. 3.52: goes on to state “The quality assurance policy and programmes for physical protection should ensure that a physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or design basis threat and that it meets the State’s regulations, including its prescriptive and/or performance based requirements.”

13. The IAEA also publish Implementing Guide NSS 10 ‘Development, Use and Maintenance of the Design Basis Threat’ [8], which details the use of a DBT as the basis for developing potential adversary scenarios, conducting performance analysis of the PPS, identifying vulnerabilities in the PPS and improving the PPS by analysing and prioritising upgrade options.

5. Advice to Inspectors

14. The UK DBT describes the malicious capabilities associated with sabotage that need to be addressed and the requirement for dutyholders to carry out VA Identification studies.

15. The Manual Forced Entry Standard (MFES) developed by the Centre for the Protection of National Infrastructure (CPNI) reflects independent forced entry testing of physical barriers to classify their performance and approve their

use for protecting UK government and national infrastructure. The standard reflects a range of threats faced by UK government and national infrastructure. In particular, this standard reflects: generic levels of knowledge and experience of those actors intelligence has shown are likely to attempt to attack and disrupt UK government and national infrastructure; availability of equipment to those likely to conduct such attacks and the methodology likely to be employed. Consequently the manual should be used by dutyholders to assist validation of claims arguments and evidence in the vulnerability assessment that the PPS meets the required outcome as defined in SyAPs Annexes C and D.

16. This TAG informs regulatory assessment of dutyholder vulnerability assessments in order to meet PPS outcomes and establishes ONR's expectations of the dutyholder. The level of ONR scrutiny is dependent on the security significance of the nuclear facility concerned.

Regulatory Expectation

17. The regulatory expectation is that the dutyholder should demonstrate within their security plan how the effectiveness of the PPS has been validated through the conduct of performance based vulnerability assessments. Such assessments could comprise one or more proven methodologies such as: force-on-force exercises; table top exercises, war gaming, simulation, computer based modelling or expert analysis.

FSyP 6 - Physical Protection Systems	Vulnerability Assessments	SyDP 6.4
Dutyholders should satisfy themselves that their physical protection system achieves the required security outcome through undertaking vulnerability assessments.		

6. Key Features of a Vulnerability Assessment

18. A submission from a dutyholder should include nine key features, which are summarised below. Subsequent sections of this guide identify specific points that can support these key features. In general terms, submissions should be:

- **Complete.** All foreseeable threats (as defined in the UK DBT) are identified and evidence provided that shows the site/plant has/will have adequate protection in place to protect them, their inventory and key supporting infrastructure against theft and sabotage. Security measures should take into account the PPS outcomes for protecting

Category I to Category IV quantities of NM/ORM against theft and the graded approach for the prevention of sabotage.

- **Clear.** Identify the associated PPS outcomes in SyAPs that need to be met, the nature and magnitude of malicious capabilities and the protection in place, or going to be put in place, to prevent or mitigate their effects. The submission should be comprehensive, understandable and clear. The basis for all assumptions, conclusions and recommendations in the submission should be given and any unresolved issues explained and/or justified. Clarity needs to extend to the correct referencing of supporting information, and it is important that the basis for the level of security portrayed in the submission is evident to all users, peer reviewers, and the regulator.

- **Rational.** Provide sensible, cogent, cohesive and logical arguments to support the conclusions. This includes the arguments and evidence in support of claims that the vulnerability assessment has been completed in accordance with regulatory expectations.

- **Accurate.** Accurately reflect the 'as is' state of the plant, equipment, processes and procedures. This includes the arguments in support of claims that the vulnerability assessment has been completed and agreed by relevant stakeholders. The performance of future measures, particularly with regard to new facilities and builds, can be modelled to show that they will deliver the necessary outcome(s).

- **Objective.** Arguments should be supported with factual evidence (e.g. documented, measurable, etc). An understanding of associated systems or processes should be established from appropriate research and development. Claims relating to the integrity or performance of engineering and technical features should be supported by evidence to show they will operate as intended and there is some redundancy designed into these features that cannot be circumvented. Thus, the link between engineering/technical and security provisions should demonstrate that the extant or revised security regime has adequate defence-in-depth, taking into account the categorisation for theft and sabotage. In the absence of directly relevant information, the use of inferred or extrapolated detail needs to be carefully substantiated. The adequacy of operational procedures, managerial controls and resources should be included in any analysis.

- **Appropriate.** Analytical methods used to substantiate security arrangements in a submission, such as Adversarial Approach Path Flowcharts/Diagrams that might be used in vulnerability assessments, should be shown to be fit for purpose with adequate verification and validation. Any assumptions that have been made should be identified and shown to be appropriate. Where security arrangements are based on previous experience, sufficient evidence should be provided to show

that equivalent principles, criteria and standards to those previously used will be applied, and that these are still relevant.

- **Integrated.** Be holistic and show clear links between any analysis and engineering/technical substantiation. It should show where these depend on internal dependencies, such as standby power or communications links and other external facilities and services, and clearly specify and/or substantiate any associated assumptions that are being made. There should be clear links in the submission to any supporting documents, standards etc.

- **Current.** Be current, concise and relevant. The initial content of a submission may change if the plant/area concerned undergoes a major modification, or a series of minor modifications, which could also have a significant cumulative effect on radiological consequences. The associated security plan may also require amendment to reflect the current state of the security regime, bearing in mind all physical, operational and managerial aspects.

- **Forward looking.** Demonstrate that assessment work done during the vulnerability assessment will be reviewed throughout the lifetime of the site/plant/area to ensure it remains valid and adequate. Revalidation of a vulnerability assessment may also be required when the DBT is reviewed.

7. Vulnerability Assessment Submission – Specific Points

19. There are a number of ways that a vulnerability assessment can be undertaken, from the use of specialist computer programmes, through adapted spreadsheets to handwritten analysis. However, all vulnerability assessments should contain certain key information including:

- **Identification of Targets.** Accurately identify buildings or facilities holding NM, ORM and those identified as Vital Areas (VAs), taking into account the NM and VA categories and associated PPS Security Posture and Outcome.

- **Confirmation of Malicious Capabilities.** Relevant malicious capabilities should be confirmed (e.g. intruders, vehicle-borne improvised explosive device, insider - theft of NM and insider - sabotage). Analysis of the insider threat is important as this threat is particularly difficult to counter given an insider has authorised access and is in a position of trust. The amendment to CPPNM (Fundamental Principles G: Threat and I: Defence in Depth) acknowledges that an integrated protection solution must be designed to minimise the likelihood of Insider attack. Insiders could be capable of using methods and opportunities that are not available to external attackers. They

have authority to access areas where the most vulnerable targets are located and may be able to choose an optimum time to attempt or perform a malicious act. Insiders have the opportunity to extend the malicious act over a long period of time to maximise the likelihood of success/lessen the risk of discovery. An insider may also be in collusion with external attackers and able to compromise the PPS, to enable access in some way, or by creating a diversionary incident. Scenario analysis (see below) should consider where an insider could act to minimise the likelihood of success for the response force and be taken in to account.

- **Scenario Analysis.** Provide a basis for the confident evaluation of the PPS design. As the attack strategy may be unknown, developing a small number of distinct, different and unique scenarios will allow the expected performance to be determined and validated. The scenarios should be credible, consistent, challenging, transparent, documented and consistent with the DBT. Scenarios should consider the possibility of a sub-optimal response by the response force; for example, by introducing an element of confusion, incapacitation or communication failures. The scenarios should comprise detailed plans of the adversary attack strategies allowing confidence to be gained in the adequacy of the physical protection system design against a variety of worst-case incidents.

- **Adversarial Approach Path Analysis.** Identify the path(s) that are the most vulnerable and, where appropriate, least likely to result in the response force interrupting the malicious activity be it theft or sabotage. This includes adversary path(s) that have the minimum likelihood of initial detection, then once detection occurs, the minimum delay time to support an effective interdiction by the response force. There are a number of methods to determine the optimum malicious attack route, but all rely upon the reaction time of the response force being known, coupled with detection and delay times. The path analysis should also identify the Primary and Critical Detection Points (PDP/CDP). The CDP is the last detection point where detection must occur to provide adequate time for the response force to interrupt the adversary attack (i.e. the last detection point where the malicious task time remaining is greater than the response force times).

- **Adversarial Approach Path Flowcharts/Diagrams.** Taking account of the analysis detailed above, a graphical representation of the PPS design layers and elements, and the routes an adversary could take through a facility to reach the target should be produced using a flowchart and/or diagram. Ideally, the PPS design should be modelled in layers around the target with each layer comprising the physical and technical elements that support the security arrangements. The associated delay and detection measures within each element should be identified.

- **Interruption Analysis.** Dutyholders on sites required to meet PPS Outcome 1 or 2 (see SyAPs Annexes C and D) must take account of any armed response force's Concept of Operations (ConOps), containment or denial strategies, pre-determined intervention points and final denial points, as appropriate when conducting Interruption Analysis. Response times should take account of the time taken for the alarm signal from a detector to be transmitted, displayed and assessed, and for it to be communicated to the response force. Interruption analysis then allows the CDP to be determined.

- **Neutralisation Analysis.** Dutyholders on sites required to meet PPS Outcome 1 will need to undertake a neutralisation analysis which incorporates a number of key factors, amongst them being the number, tactics and weapons of both the adversary and the armed response force. Adversarial capabilities are detailed in the DBT document and the armed response force capabilities should be included in a ConOps. Several methodologies can be used to determine the likely probability of the armed response force preventing the adversary carrying out a malicious act (theft or sabotage) against the target including:
    - expert opinion;
    - table top analysis;
    - numerical methods such as Markov Chain[1];
    - computer simulations and modelling;
    - force on force exercises; and
    - operational experience from real engagements.

- **Real world performance considerations.** Irrespective of the method used it should be borne in mind that the adversary will initially have the initiative, as they can determine the time and location of the attack, know their plans and the likely strengths and weaknesses of their strategy, and may have insider assistance. The response force will initially respond to a developing incident rather than commanding the situation. The posture of the response force, "pre-event", should be realistic and analysis of historical response force locations/deployment data should be used. This includes unarmed response forces, who may be dispatched to verify alarms in support of achieving a PPS outcome.

[1] A Markov Chain is a mathematical system that undergoes transitions from one state to another, between a finite or countable number of possible states. It is a random process where the next state depends only on the current state and not on the sequence of events that preceded it. Markov chains have many applications as statistical models of real-world processes.

- **Identify Potential Vulnerabilities.** Taking the above into account, identify the potential vulnerabilities in existing security arrangements that need to be considered in the submission.

- **Produce Vulnerability Assessment Submission.** Produce the submission ensuring all risks are recorded for validation by ONR.

20. The submission should be examined by an ONR security inspector(s) with a comprehensive knowledge of the site's infrastructure and operations. Foremost, is the need to examine evidence in a dutyholder's submission to support claims and arguments that adequate measures are in place, or are going to be put in place, to protect against theft and sabotage, and achieve relevant PPS outcomes detailed in the SyAPs. Where required, ONR security inspectors should seek additional information to support dutyholder's claims, particularly if evidence appears to be missing from a submission or is inadequate to support a claim. If the evidence is available it should be included in an updated submission. If the evidence is not available further work will be required by the dutyholder to substantiate their claims.

21. An administrative process for dealing with vulnerability assessment submissions is included in the ONR How2 management system. However, the key features detailed in Section 7 above should be found in all submissions forwarded to ONR for validation.

22. The dutyholder is responsible for the production of a vulnerability assessment submission. However, others, such as the armed response force or guard force who have direct responsibility for delivering security, should be involved in the submission and have a comprehensive understanding of it.

8. Peer Review, Assurance and Governance

23. During the production process, a vulnerability assessment submission should undergo an internal peer review, including an assurance and governance process by suitably qualified security and operational staff before it is submitted. As part of the approval process for a submission it is important that:

- appropriate methods and relevant security standards and specifications have been used, and the calculations that have been used are correct and assumptions realistic;

- where necessary, there has been independent verification or advice by suitably qualified and experienced staff, including the armed response force (to verify performance aspects), CPNI, and Centre for Applied Science and Technology (for physical and technical security equipment performance);

- other third parties involved can demonstrate their competence to undertake such work and evidence that where they have raised challenges these have been addressed; and,
- the vulnerability assessment is complete, all key security assumptions are valid, and the Board member (or equivalent) for security has been briefed on all aspects of the vulnerability assessment and has endorsed the approach used for its production.

Inspectors should consider

- Does the vulnerability assessment incorporate the nine key features of a good submission?
- Does the vulnerability assessment accurately reflect all buildings and facilities as categorised by target identification for theft and sabotage processes detailed in SyDPs 6.1 and 6.2?
- Is the vulnerability assessment based on all relevant malicious capabilities described in the DBT document and has adequate consideration been given to the insider threat?
- Does the vulnerability assessment include scenario analysis that is credible, challenging, transparent and considers the possibility of sub-optimal performance by the response force?
- Does the vulnerability assessment include adversarial path analysis that identifies the most vulnerable paths and utilises accurate detection and delay times?
- Does the vulnerability assessment include aspects such as graphical representation, modelling, flow charts or diagrams to assist understanding and interpretation?
- Where the PPS is required to achieve Outcome 1 or 2, does the vulnerability assessment incorporate interruption analysis?
- Where the PPS in required to achieve Outcome 1, does the vulnerability assessment incorporate neutralisation analysis?
- Does the vulnerability assessment incorporate real world performance considerations of armed and unarmed response force capabilities?
- Does the vulnerability assessment record all potential vulnerabilities in the PPS and any associated risks?
- Has the vulnerability assessment been subject to appropriate internal assurance and Governance arrangements?

9. Vulnerability Assessment Submission

24. Once completed, dutyholders are expected to submit completed vulnerability assessments to ONR for validation. The submission should support and confirm that the effects required from the PPS are met or justify the reasons why this is not the case.

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, “Nuclear Security Series No. 10. Nuclear Security Recommendations on Radioactive Material and Associated Facilities”.

Glossary and Abbreviations

CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CDP	Critical Detection Point
DBT	Design Basis Threat
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
PDP	Primary Detection Point
PPS	Physical Protection System
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
VA	Vital Area
VAI	Vital Area Identification