



ONR GUIDE			
GUIDANCE ON THE PURPOSE, SCOPE AND QUALITY OF A NUCLEAR SITE SECURITY PLAN			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-001 Revision 1		
Date Issued:	March 2016	Review Date:	March 2019
Approved by:	Angus Cameron	Superintending Inspector	
Record Reference:	TRIM Folder 1.9.3.936. Unique Ref: 2016/0120708		
Revision commentary:	Document rebranded and minor content updates		

TABLE OF CONTENTS

1.	INTRODUCTION.....	3
2.	PURPOSE AND SCOPE	3
3.	RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION.....	3
4.	RELATIONSHIP TO OTHER SECURITY GUIDANCE AND POLICY DOCUMENTS	3
5.	ADVICE TO INSPECTORS	4
6.	NUCLEAR SITE SECURITY PLAN	4
7.	KEY FEATURES OF A NUCLEAR SITE SECURITY PLAN.....	4
8.	STRUCTURE AND APPLICATION OF THE NUCLEAR SITE SECURITY PLAN.....	6
9.	NUCLEAR SECURITY CASE - PART ONE OF THE NSSP	6
	Introduction	6
	Mission Statement.....	6
	Content of a Nuclear Security Case.....	6
10.	INTEGRATED PROTECTION SOLUTION - PART TWO OF THE NSSP	8
	Introduction	8
	Content of an Integrated Protection Solution	8
11.	ADJACENT CIVIL NUCLEAR LICENSED SITES.....	9
12.	OWNERSHIP, MANAGEMENT AND MAINTENANCE OF NUCLEAR SITE SECURITY PLANS	9
13.	PRODUCTION, REVISION AND REVIEW OF NUCLEAR SITE SECURITY PLANS.....	9
14.	PEER REVIEW, ASSURANCE AND GOVERNANCE.....	9
15.	SUBMISSION OF A NUCLEAR SITE SECURITY PLAN	10
16.	ALTERNATIVE ARRANGEMENTS TO MODEL SECURITY STANDARDS	10

17. SECURITY CULTURE	10
18. REFERENCES.....	11
19. GLOSSARY AND ABBREVIATIONS	12
20. APPENDICES	13
Appendix 1: Extract of Regulations from NISR 2003	13
Appendix 2: Example of the type of information for inclusion in the Integrated Protection Solution	16

© Office for Nuclear Regulation, 2016

If you wish to reuse this information visit www.onr.org.uk/copyright for details.

OFFICIAL

OFFICIAL

1. INTRODUCTION

1.1. The Office for Nuclear Regulation (ONR) has established a set of National Objectives, Requirements and Model Standards (NORMS) that dutyholders must demonstrate they have been fully taken into account in developing their security regime. The security regime for meeting NORMS is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations 2003. NORMS is supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1. This Technical Assessment Guide (TAG) contains guidance to advise and inform Security Inspectors in the Office for Nuclear Regulation in the exercise of their regulatory judgement. It aims to provide general advice and guidance to ONR staff on how to assess the adequacy of a dutyholder's Nuclear Site Security Plan (NSSP) and the arrangements for their production (see paragraphs 13.1 to 13.3) and management. It does not set out how ONR regulates these arrangements, or provide examples of the detailed information that a NSSP should contain.

2.2. The term 'Dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil licensed nuclear sites and other (unlicensed) nuclear premises subject to regulation, as defined in the Nuclear Industries Security Regulations (NISR) 2003 (References 1 and 2). It is also used to refer to a 'licensee' as defined in paragraph 1 of a Nuclear Site Licence granted under the provisions of the Nuclear Installations Act 1965, or a 'developer' carrying out work on a nuclear construction site, as described in the Nuclear Industries Security (Amendment) Regulations 2012 (Reference 3)¹.

2.3. As this guide will be used by ONR security inspectors to consider the adequacy of a dutyholder's NSSP, it indicates to dutyholders and other stakeholders the standards that ONR expects. It is intended that this guide will influence the issues that should be addressed in NSSPs. The guide does not prescribe the detail or the depth that needs to be addressed; these remain the responsibility of the dutyholder and will be dependent upon the specifics of each NSSP.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

3.1. The NISR 2003 (as amended) defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan (i.e. NSSP) in accordance with Regulation 4, replace or amend a security plan in accordance with Regulation 6 and maintain security that complies with the approved standards, procedures and arrangements, as detailed in Regulation 7. Regulation 8 also covers the requirement for Temporary Security Plans (TSPs). Relevant extract(s) from these Regulations are reproduced in Appendix 1 for information.

3.2. Throughout a site's lifecycle, the security arrangements in place, together with their rationale are to be detailed in an approved NSSP. Where necessary, Temporary Security Plans (TSPs) or Temporary Security Arrangements (TSAs) will be submitted as detailed in the NORMS document. Other exceptions are only permitted for unforeseen security events, or other emergencies when rapid responses are needed for security/safety purposes. Such events should be rare, and are to be dealt with, where appropriate, in accordance with extant CT/Security Event Contingency Plans.

4. RELATIONSHIP TO OTHER SECURITY GUIDANCE AND POLICY DOCUMENTS

4.1. The IAEA document INFCIRC225 Revision 5 (Reference 4) at paragraph 3.27, supporting Fundamental Principle E: Responsibility of the License Holders, recommends that 'license holders'

¹ Not yet in force at 29 November 2012

OFFICIAL

should prepare a 'security plan' based on the 'threat assessment' or the 'design basis threat' including sections dealing with design, evaluation, implementation and maintenance of the physical protection system and contingency plans. The 'competent authority' should review and approve the security plan.

4.2. For the purposes of this guidance the 'license holders' are dutyholders, the 'security plan' is the NSSP, and the 'competent authority' is ONR..

4.3. The 'threat assessment/design basis threat' is detailed in the extant version of the Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) document (Reference 5)

4.4. Part One of the National Objectives, Requirements and Model Standards (NORMS) documents (Reference 6) requires that dutyholders produce NSSPs, consisting of two parts; the Nuclear Security Case (NSC) (see Section 9) and the Integrated Protection Solution (IPS) (see Section 9).

4.5. The HMG Security Policy Framework (SPF) (Reference 7), issued by the Cabinet Office, is adopted by the whole of the civil nuclear industry for the protection of Sensitive Nuclear Information (SNI) and the employment of appropriate personnel security controls on and off nuclear premises.

4.6. The NISR Classification Policy (Reference 8) indicates those categories of SNI that require protection and the level of protective marking to be applied.

5. ADVICE TO INSPECTORS

5.1. The judgement of ONR Security Inspectors is required in deciding whether to approve or reject a NSSP. An administrative process for this is included in the ONR How2 management system. However, the key features detailed at Section 7 should be found in all NSSPs.

5.2. The evidence to support the claims and arguments, particularly in the NSC, that the security objectives are being met must be present. Where this evidence is missing from the NSSP then Inspectors should seek additional information to support the dutyholder's assertions and this should be included in an updated NSSP.

5.3. It should be remembered that the approved NSSP will form the basis for compliance inspection activities by ONR Security Inspectors.

6. NUCLEAR SITE SECURITY PLAN

6.1. For ONR security regulatory purposes, Part One of a NSSP is to comprise the NSC (see paragraphs 9.1 to 8.11) and Part Two of the NSSP is to contain the IPS (see paragraphs 10.1 to 10.7). As integral elements of the NSSP, both the NSC and IPS are part of the formal approval process, required in accordance with the NISR 2003, Regulation 4.

7. KEY FEATURES OF A NUCLEAR SITE SECURITY PLAN

7.1. A good NSSP should include nine key features, which are summarised below. Subsequent sections of this guide translate these key features into more specific points. The NSSP should be:

- a. **Complete.** Foreseeable threats (as defined in the NIMCA document) to security should be identified and it should be shown that the site/plant has adequate protection in place to counter relevant malicious capability. This should include, where necessary, the mitigation of geographical features on and surrounding a site, that could undermine the effectiveness of the security force. The security measures in place should also take into account the Categorisation Tables for theft and the graded approach for the prevention of sabotage, as detailed in Parts Two and Three of the NORMS document.

OFFICIAL

OFFICIAL

- b. **Clear.** The NSSP should highlight the key points in terms of both strengths and weaknesses. There should be a clear statement as to the security objectives that need to be met, the nature and magnitude of the significant malicious capabilities and the protection in place to prevent or mitigate their effects. The NSSP needs to be readily accessible as well as understandable. It should be possible to navigate easily around the NSSP to find relevant information. The basis of all assumptions, conclusions and recommendations should be given and any unresolved issues explained and justified. Clarity needs to extend to the correct referencing of supporting information. It is important that the basis for the level of security portrayed in the NSSP is evident to all users, including the regulator.
- c. **Rational.** The NSSP should be reasonable and sensible. It should provide cogent, cohesive and logical arguments to support the conclusions. This includes the arguments in support of claims that risks have been reduced so far as is reasonably practicable.
- d. **Accurate.** The NSSP should accurately reflect the 'as is' state of the plant, equipment, processes and procedures.
- e. **Objective.** The arguments developed in the NSSP should be supported with factual evidence (i.e. documented, measurable, etc.). The necessary understanding of the behaviour of systems or processes should be established from appropriate research and development. Claims relating to the integrity or performance of engineering/technical features should be supported by relevant documents having been assessed/tested where possible to ensure there are no gaps, or opportunities for circumvention. Thus, the link between engineering/technical and security provisions should be demonstrated in line with the requirements for a security regime that has defence-in-depth. In the absence of directly relevant information, the use of inferred or extrapolated detail needs to be carefully substantiated. There is a need to provide visibility of the sensitivity to assumptions to validate the robustness of associated claims. The adequacy of operational procedures, managerial controls and resources should be demonstrated by analysis to an appropriate level.
- f. **Appropriate.** Any analytical methods used to substantiate security arrangements, such as those that may be used during Vulnerability Assessment, 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 is demonstrated using claims based on previous experience, sufficient evidence should be presented to show that equivalent principles, criteria and standards to those previously used have been applied, and that existing information is relevant to any new facility.
- g. **Integrated.** The NSSP should be holistic so that there are clear links between any security analysis and engineering/technical substantiation. It should also define where it depends on other external facilities and services, for example standby power/UPS, and clearly specify and substantiate any associated assumptions that are being made. There should also be clear links in the NSSP to operational requirements and any constraints that may need to be considered as detailed in associated documents.
- h. **Current.** The NSSP must be reviewed, revised and updated to ensure it remains current, concise and relevant. As the site/plant passes through its life cycle, the NSSP should be reviewed to ensure it remains valid. The content of a NSSP may also change if the site/plant undergoes a major modification, or a series of minor modifications, which have a significant cumulative effect on security. The NSC and IPS are subject to amendment to reflect the current state of the security regime bearing in mind all physical, operational and managerial aspects.
- i. **Forward looking.** The NSSP should demonstrate that the site/plant will remain safe and secure throughout a defined lifetime.

OFFICIAL

OFFICIAL**8. STRUCTURE AND APPLICATION OF THE NUCLEAR SITE SECURITY PLAN**

8.1. The dutyholder should produce a NSC and an IPS based on site-specific considerations, which includes all relevant information necessary to show security arrangements are adequate. They should provide evidence that the site/plant/area is as secure as is reasonably practicable. The application of the requirements identified in the NSSP should result in:

- a. an effective and proportionate security system;
- b. a clear specification for the purpose, standards and expectations of each element in the NSC;
- c. identified ways to monitor and test the security system to ensure each element functions to the required specification or standard;
- d. the production of operating and maintenance instructions, including contingency plans, to sustain the integrity of the security system;
- e. clearly defined training requirements, and the qualifications needed for specific roles and posts identified within the NSC; and
- f. an effective system of review to ensure any significant issue that arises is considered promptly to allow for continuous improvement of a site's security regime.

9. NUCLEAR SECURITY CASE - PART ONE OF THE NSSP**Introduction**

9.1. The NSC should justify the claims, arguments and rationale for the dutyholder's security regime by substantiating the security arrangements for a site, plant, activity, operation or modification. It should provide written evidence that the relevant security standards have been or are going to be met. It should also demonstrate that the risk posed by malicious activity has been reduced as far as could be reasonably expected.

9.2. The following paragraphs contain guidance for ONR inspectors to assist when making an assessment of the adequacy of a NSC prepared by dutyholders, specifically to explain the rationale for the security regime detailed in the NSSP.

9.3. The term NSC may relate to a site or part thereof, a specific plant, or part of a plant, a plant modification, or a set of significant issues.

Mission Statement

9.4. The NSC should include a statement describing a site's mission to provide a security regime. For example, to protect Nuclear Material (NM), any other Vital Areas (VAs), Other Radioactive Material (ORM) (including radioactive sources and waste) and Sensitive Nuclear Information (SNI) held on site against sabotage, theft and any other malevolent or criminal act in order to maintain site safety and retain public confidence.

9.5. Any dutyholder security policies that support or deliver the mission and impact on the implementation of security arrangements should also be referenced in the NSC.

Content of a Nuclear Security Case

9.6. A NSC is intended to demonstrate that the dutyholder has taken into account all relevant issues when planning the security of their site. It should identify key protective security assets, the capability and resilience of security equipment, the competence of those specifying, installing, operating and maintaining the security system, and of those providing a response to any relevant

OFFICIAL

OFFICIAL

malicious capabilities given in the NIMCA document. The contents of a NSC are detailed further in the following paragraphs and should typically be expected to:

- a. identify the dutyholder's parent company and site specific security organisation(s) along with details on the use of company, contract and police resources for security, detailing how they will be integrated to ensure complete coverage, clear responsibility and primacy;
- b. detail current plant status, site operations and function (including reactor type and number where applicable or process and storage buildings as appropriate), its size, layout and geographical location;
- c. provide a description of the site and facilities with an outline of future site plans, committed or planned, with particular reference to specific key assets that require protection. This should include future material changes to the site inventories, future strategies, such as time to decommissioning and any other factors that may subsequently affect the risk profile of the site;
- d. provide details, including the categorisation (for physical protection purposes), of the holdings of NM and ORM (including radioactive sources) for which the dutyholder is responsible. It should also detail any plans to reduce the site's NM/ORM inventory, allowing time at risk to be taken into account in justification arguments;
- e. refer to extant security enhancements contained within the Security Improvement Schedule (SIS) (as part of the NSSP) or any proposed changes. Arrangements may include physical assets, personnel resources, including the Civil Nuclear Constabulary (CNC), electronic systems, procedures and processes to describe the operational arrangements and those for maintenance of equipment. An assessment of the capital investment necessary to replace or refresh assets should be made and be able to support the continued availability of the security infrastructure;
- f. reference and consider relevant malicious capabilities contained in the NIMCA document taking into account the categorisation of material for theft and the graded approach for the prevention of sabotage. This should include the identification of key assets to be protected and designation of site risks, including the requirement for VA Identification and protection;
- g. detail the findings of Vulnerability Assessments or, as required, a Gap Analysis (see the NORMS document) of existing security arrangements. It should be explained which malicious capabilities have been considered and how any identified security vulnerabilities are mitigated, removed, minimised or controlled;
- h. refer to relevant security objectives detailed in the various parts of the NORMS document and detail any optioneering undertaken to identify alternative methods to model security standards that provide a commensurate degree of physical protection. A justification of the options chosen together with a programme to demonstrate the timely delivery of the changes identified should be provided;
- i. provide details of all identified VAs and the potential consequences of a successful sabotage attack on these and other key assets, including essential plant for site operations and Command, Control, Communication and Intelligence (C3I) facilities;
- j. demonstrate that the dutyholder is able to maintain the integrity of the security regime, as detailed in the NSSP, and so give the Regulator confidence in the dutyholder's ability; and
- k. describe the philosophy that underpins the maintenance and testing requirements for the security system.

OFFICIAL

OFFICIAL

9.7. The interface between the different elements of the security infrastructure should be identified in the NSC. It should also describe how elements of the security regime are integrated into the overall site emergency arrangements and procedures.

9.8. The NSC also forms the basis for the delivery of secure operations and it should identify the measures that ensure a robust culture and that security standards are maintained. These measures might include the provision of adequate operating rules and instructions; examination, maintenance and testing requirements for the security system and essential supporting equipment, such as standby power/uninterruptable power supplies (UPS); maintaining minimum staffing levels in key areas and providing appropriate staff training and effective contingency plans/procedures.

9.9. From construction of the site through to decommissioning, there may be various key stages that require special consideration. In these instances, the NSC should demonstrate that any changes in security arrangements are considered proportionate to manage the risk and counter any relevant malicious capabilities at the time.

8.10. It follows that the NSC is also subject to review, change and amendment. For example, it may change due to significant changes to a site, plant, its operation and/or any change in its life cycle, or a change in security related issues. It may also change in the light of operating experience.

8.11 On the more complex sites, a dutyholder may choose not to include all operations that may affect security on a site in a single NSC, but instead produce separate NSCs for specific plants, operations or parts of a site. In this event, the separate NSCs should demonstrate that they are adequately integrated as part of the overall security regime (e.g. using common services for C3I and contingency arrangements) and any integration required for safety and security interfaces.

10. INTEGRATED PROTECTION SOLUTION - PART TWO OF THE NSSP**Introduction**

10.1. An IPS provides information that details the physical, technical, personnel and associated security measures and procedures for the dutyholder's security regime. Therefore, it should describe the integrated security arrangements for a site and/or specific plant and provide written evidence of respective security standards in place, or to be provided.

10.2. The following paragraphs contain guidance for CNS inspectors to assist when making an assessment of the adequacy of an IPS prepared by dutyholders, specifically to detail the rationale for the security regime as detailed in the NSC.

10.3. The term IPS relates to the site as a whole, including specific details for plant(s), part of a plant(s), or a set of significant issues.

Content of an Integrated Protection Solution

10.4. The IPS should provide a comprehensive description and demonstrate understanding of how all aspects of the protective security regime are integrated, in order to ensure a holistic and effective security framework.

10.5. Where the security standards detailed in the IPS differ from the model security standards laid down in the NORMS document, the dutyholder must be able to demonstrate that they provide a commensurate level of physical protection and are able to achieve the relevant security objectives detailed in the NORMS document.

10.6. Area headings that could be covered in the IPS are provided in Appendix 2, at an OFFICIAL level and more specific information on the security measures that may be considered in the IPS are listed separately in Appendix 3, which is security classified as OFFICIAL - SENSITIVE due to its overall content.

OFFICIAL

OFFICIAL

10.7. The IPS is subject to review, change and amendment. For example, the security arrangements may change due to important changes to a plant, its operation and/or any change in its lifecycle, or to take into account a change in a security related issue. It may also change in the light of operating experience.

10.8. Projects or tasks that are required to bring the security arrangements on the site up to the standard required are to be detailed in the SIS as an annex to the NSSP with information on the scope and schedule

11. ADJACENT CIVIL NUCLEAR LICENSED SITES

11.1. Where a civil nuclear licensed site is adjacent to, or forms an enclave within another licensed site, then both dutyholders must give consideration in their NSC and IPS to any shared services or shared contingency/emergency arrangements and to the impact that one may have, as an external hazard, on the other. Adequate arrangements need to be made to ensure that information is shared to enable the above considerations to be taken into account. The dutyholder must be able to demonstrate a coherent, coordinated approach is being maintained.

12. OWNERSHIP, MANAGEMENT AND MAINTENANCE OF NUCLEAR SITE SECURITY PLANS

12.1. The dutyholder is legally responsible for the production of a NSSP. However, others such as the CNC and those employees of the dutyholder who have direct responsibility for delivering security should also have 'ownership' of it. This means having an understanding of the NSC, and the IPS, and the limits and conditions derived from it.

13. PRODUCTION, REVISION AND REVIEW OF NUCLEAR SITE SECURITY PLANS

13.1. The responsibilities for production, revision, and review of NSSPs and overall document control should be clearly defined and detailed in the NSSP, as part of compliance arrangements. Suitably qualified and experienced people should discharge these responsibilities. Where the dutyholder itself does not develop all aspects of the NSC and uses contractors for this purpose, at all times the dutyholder must possess (in-house) the technical capability to understand all aspects of the NSC(s) and the IPS.

13.2. It is important that a NSSP is kept up to date and periodic reviews of the NSC and IPS are undertaken (the frequency of which should be determined by the dutyholder). Significant changes may occur during operations such as modification, incidents, revised lifetime plans, etc. Such changes should be recorded and taken forward as necessary in an updated NSC and IPS, which accurately reflects the current situation.

13.3. Documentation which no longer forms part of a current NSSP, or which has been superseded, should be identified and archived. This information still forms part of the formal historical record, and should remain available for reference by the dutyholder, security staff and ONR.

14. PEER REVIEW, ASSURANCE AND GOVERNANCE

14.1. As part of the production process, a NSSP should undergo an internal peer review and be subject to an assurance and governance process by suitably qualified security and operational staff. As part of the approval process for an NSSP it is important to ensure that:

- a. appropriate methods and relevant security standards and specifications have been used where appropriate and the calculations that have been used are correct;
- b. the site/plant and operational details documented are consistent with the actual site/plant and its operations;

OFFICIAL

OFFICIAL

- c. where considered necessary, there has been independent verification or advice provided by suitably qualified and experienced staff, such as those employed by CPNI, SSG and CAST;
- d. where there has been other third party involvement there is evidence of their competence to undertake their work and evidence that where they have raised challenges these have addressed and the NSSP improved accordingly;
- e. any available evidence from the dutyholder's internal audit function should confirm that the NSSP has been produced in compliance with relevant company procedures for the production of security plans; and
- f. the NSC and IPS are complete, all key security assumptions are valid and the board member (or equivalent) for security has been briefed on all aspects of the plan and has endorsed the approach used for its production.

15. SUBMISSION OF A NUCLEAR SITE SECURITY PLAN

15.1. Once completed, dutyholders are expected to submit a NSSP to ONR for approval to an agreed programme. The NSC should justify the security measure(s) required to achieve the relevant security objectives in the NORMS document, or explain why another approach is justified. The IPS should describe those measures.

16. ALTERNATIVE ARRANGEMENTS TO MODEL SECURITY STANDARDS

16.1. The onus is on the dutyholder to justify any alternative arrangements from the model security standards given in the NORMS document, to achieve the required security objective(s), by producing a proposal for consideration and assessment by ONR. The content and scope of the proposal, and the impact on the NSSP will depend on the extent to which a dutyholder is proposing to deviate from the model security standards for protecting NM/ORM from theft or sabotage. The proposal, detailed in the NSC should detail the dutyholder's claims for the security regime they propose putting/having in place. It should also provide supporting information to justify how any alternative security measure(s) in the IPS meets the security objectives, together with any further evidence necessary to support their case. As mentioned previously, irrespective of the size or scope of the proposal, it will need to be complete, clear, rational, accurate, objective, appropriate, current and forward-looking.

17. SECURITY CULTURE

17.1. The NSC should be used as a vehicle to improve security culture and enable staff to be made aware (via provision of appropriate training) of the security significance of the site and specific plant areas. The dutyholder should use, as far as possible, its own staff in the production and maintenance of security documentation and it should make the whole NSC available to appropriate staff on a strict need-to-know basis.

OFFICIAL

OFFICIAL**18. REFERENCES**

1. **Nuclear Industries Security Regulations 2003.** Statutory Instrument 2003 No. 403
2. **Nuclear Industries Security (Amendment) Regulations 2006.** Statutory Instrument 2006 No. 2815
3. **Nuclear Industries Security (Amendment) Regulations 2013.** Statutory Instrument 2013 No. 190
4. IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
5. **Nuclear Industries Malicious Capabilities Planning Assumptions.** 9 July 2012.
6. **National Objectives, Requirements and Model Standards.** October 2012. Trim Folder 4.4.2.10321.
7. **HMG Security Policy Framework.**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf
8. **NISR Classification Policy** – Information concerning the Use, Storage and Transport of Nuclear and Other Radioactive Material. Office for Nuclear Regulation. Version 7.1 January 2014 TRIM Ref: 2014/9790

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

OFFICIAL

19. GLOSSARY AND ABBREVIATIONS

C2	Command and Control
C3I	Command, Control, Communication and Intelligence
CAST	Home Office Centre for Applied Science and Technology
CNC	Civil Nuclear Constabulary
CNS	Civil Nuclear Security
IDS	Intruder Detection System
IPS	Integrated Protection Solution
MOU	Memorandum of Understanding
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NORMS	National Objectives, Requirements and Model Standards
NSC	Nuclear Security Case
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PIDS	Perimeter Intruder Detection System
SIS	Security Improvement Schedule
SNI	Sensitive Nuclear Information
SSG	Defence Estates Special Services Group
TAG	Technical Assessment Guide
TSA	Temporary Security Arrangement
TSP	Temporary Security Plan
VA	Vital Area
VAI	Vital Area Identification

OFFICIAL**20. APPENDICES****Appendix 1: Extract of Regulations from NISR 2003**

A definition from Regulation 2(1) and Regulations 4, 6, 7 and 8 are reproduced below.

Regulation 2 (1)

“nuclear premises” means -

- (a) a nuclear site on which nuclear material or other radioactive material is used or stored;
 - (b) premises that form part of a nuclear site are premises on which a person, who is not the holder of the nuclear site licence and is not acting as an officer, employee or contractor of that holder, uses or stores nuclear material or other radioactive material; or
 - (c) other nuclear premises on which Category **I/II** nuclear material or Category **III** nuclear material is used or stored, but excluding premises that are used solely for the purpose of the temporary storage of such material during the course of or incidental to its transport in any case where the standards, procedures and arrangements in respect of the security of transport are contained in an approved transport security statement
- (2) “Responsible person”, in relation to any nuclear premises, means -
- (a) in the case of a nuclear site falling within paragraph (a) of the definition of “nuclear premises”, the holder of the nuclear site licence;
 - (b) in the case of premises falling within paragraph (b) of that definition, the person mentioned in that paragraph; and
 - (c) in the case of premises falling within paragraph (c) of that definition, the person who uses or stores the Category **I/II** nuclear material or Category **III** nuclear material on those premises, but this is subject to paragraph (3).
- (3) No person is the responsible person in relation to any nuclear premises falling within paragraph (b) or (c) of the definition of “nuclear premises” by virtue of using or storing nuclear material or other radioactive material on behalf of another person if he is that other person’s officer, employee or contractor.

Regulation 4: Requirement for approved security plan for nuclear premises:

- (1). There must be an approved security plan for each nuclear premises (whether or not the premises form part of other premises to which this paragraph applies).
- (2). A security plan must describe in writing the standards, procedures and arrangements adopted or to be adopted by the responsible person to ensure the security of –
 - (a) the nuclear premises in relation to which he is the responsible person,
 - (b) any Category **I/II** nuclear material and Category **III** nuclear material used or stored on the premises,
 - (c) any equipment used or stored on the premises in connection with activities involving nuclear material,
 - (d) any sensitive nuclear information kept on the premises, and

OFFICIAL

OFFICIAL

- (e) in the case of nuclear premises which are or form part of a nuclear site –
 - (i) any nuclear material (so far as not already mentioned in subparagraph (b)) and other radioactive material used or stored on the premises, and
 - (ii) any equipment used or stored on the premises in connection with activities involving other radioactive material.
- (3). In particular, but without prejudice to the generality of paragraph (2), the plan must describe the standards, procedures and arrangements relating to –
- (a) the investigation and assessment by the Secretary of State of the suitability of relevant personnel of the responsible person with a view to ensuring the security of the premises and the material, equipment and information mentioned in paragraph (2);
 - (b) the receipt and despatch of any Category I/II nuclear material and Category III nuclear material to be transported to or from the nuclear premises;
 - (c) 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; and
 - (d) the steps to be taken by the responsible person or any person acting on his behalf if any event of a kind specified in regulation 10(5)(a), (b), (e) or (h) that requires immediate action occurs, and the regular practice of the activities required in connection with those steps.

Regulation 6: Replacement, amendment and revocation of approved security plans

- (1). The responsible person in relation to each nuclear premises may at any time submit to the Secretary of State for approval -
 - (a) a fresh security plan for the premises, or
 - (b) proposals for amending the approved security plan for the premises.
- (2). The Secretary of State may approve the plan or proposals as submitted or with such amendments as she may require.
- (3). On approving a fresh security plan for the premises, the Secretary of State may revoke the approval of the former plan for the premises.

Regulation 7: Maintenance of security

- (1). The responsible person in relation to each nuclear premises must comply with the standards, procedures and arrangements described in the approved security plan for the premises.
- (2). The responsible person is not to be regarded as having failed to comply with any of those standards, procedures or arrangements by reason of any matter if the Secretary of State has notified the responsible person in writing that that matter, or a matter of its description, is in her opinion unlikely to be prejudicial to the security of

OFFICIAL

OFFICIAL

the premises and the material, equipment and information mentioned in regulation 4(2)

Regulation 8: Temporary Security Plan during building works etc

(1). If it is proposed to carry out any work of alteration or extension to any building or other structure which is, or forms part of, nuclear premises -

(a) the responsible person in relation to the premises must give notice in writing to the Secretary of State -

(i) specifying the nature of the proposed works, and

(ii) stating whether in his opinion they are likely to involve any derogation from any of the standards, procedures and arrangements described in the approved security plan for the premises, and

(b) the works may not be begun until the Secretary of State has approved a temporary security plan for them.

(2). Paragraph (1) does not apply in the case of any particular work if before the work is begun the Secretary of State has notified the responsible person in writing that that work, or any work of a description that includes that work, is in her opinion unlikely to be prejudicial to the security of the premises and the material and equipment mentioned in regulation 4(2).

(3). To obtain approval of a temporary security plan for any works, the responsible person must submit the plan in writing to the Secretary of State.

(4). The temporary security plan must describe any standards, procedures and arrangements which the responsible person proposes to adopt to ensure the security of the premises and the material and equipment mentioned in regulation 4(2) during the period whilst the works are being carried out.

(5). The Secretary of State may approve the temporary security plan as submitted or with such amendments as she may require.

(6). During the period whilst the works are being carried out, the approved security plan for the premises has effect subject to the approved temporary security plan.

(7). During that period the responsible person must comply with the standards, procedures and arrangements described in the approved temporary security plan.

(8). The responsible person may at any time submit proposals for amending the approved temporary security plan to the Secretary of State, and the Secretary of State may approve the proposals as submitted or with such amendments as she may require.

(9). In the case of premises which are nuclear premises on the commencement date, paragraphs (1) to (8) of this regulation do not apply until there is an approved security plan for the premises.

OFFICIAL

OFFICIAL**Appendix 2: Example of the type of information for inclusion in the Integrated Protection Solution****Introduction**

1. This non-protectively marked Appendix provides an example of the type of information that should be included in the IPS section of a NSSP. The aim of this appendix is to assist in ensuring that a consistent approach is maintained across the assessment regime. It is also to provide a readily accessible indication, at a non-protectively marked level, of examples of those areas that should be covered within an IPS.

2. The onus always lies with the Dutyholder to explain, demonstrate and, where appropriate, provide evidence, that the security arrangements detailed in an IPS follow from the NSC and that it is the result of a detailed analysis of the threat and how the threat can best be mitigated. The typical content set out below should not be considered exhaustive as each NSC and IPS will be different, and there could be other factors to consider. The details will need to be tailored to the nature of the site, plant or facility. Security measures which should be considered in the IPS include:

3. **The Management of Security**

Security Organisation and Roles

Security Culture

Audit Procedures

Security Performance Assessment

4. **The Security Arrangements**

Holdings of Nuclear Material (NM) and Other Radioactive Material (ORM)

Physical Security Measures including:

Nuclear Premises Perimeter

Perimeter Gatehouses (s)

High Security Area Perimeter (if appropriate)

Inner Areas/Vital Areas (if appropriate)

Buildings, Stores and Other Areas holding Category III nuclear material

Command, Control, Communication and Intelligence including:

Main Control Room (MCR)/Central Control Room (CCR) on Nuclear Power Stations, Station Security Control Room (SSCR)/Police Control Room (PCR)

OFFICIAL

OFFICIAL

Access Control Measures covering:

Perimeter Gatehouse(s)

Other Perimeter Access Points

Access Control Procedures through Perimeter

High Security Area Access Control (if appropriate)

Information Security

Personnel Security

Transport Security

Incident Management

Security Forces

5. **The Maintenance of Security**

Audit and Testing Procedures

Training

Repair and Maintenance

OFFICIAL