



ONR GUIDE			
GUIDANCE ON THE ASSESSMENT OF A DUTYHOLDER’S SECURITY PERFORMANCE			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-015 Revision 0		
Date Issued:	August 2014	Review Date:	August 2017
Approved by:	Tom Parkhouse	Superintending Inspector	
Record Reference:	TRIM Folder 1.9.3.740. (2014/0177179)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP WITH RELEVANT LEGISLATION.....	3
4. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS	3
5. ADVICE TO INSPECTORS – COLLECTION AND ANALYSIS OF EVIDENCE	4
6. ADVICE TO INSPECTORS – PRODUCTION OF ASSURANCE REPORT	11
7. REFERENCES	13
8. GLOSSARY AND ABBREVIATIONS	14

1. INTRODUCTION

- 1.1 The Office for Nuclear Regulation (ONR) has established security objectives for dutyholders to meet. These objectives are detailed in the National Objectives, Requirements and Model Standards (NORMS) (Reference 4) document, which describes how the objectives might be achieved through a set of requirements and model standards; although other security arrangements may be applied provided the dutyholder can demonstrate to ONR that these alternative arrangements meet the objectives. The security regime for meeting these objectives is described in the Nuclear Site Security Plans (NSSPs) prepared by dutyholders, which are approved by ONR. 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 Guide (TAG) is such a guide.

2. PURPOSE AND SCOPE

- 2.1 One of the roles of ONR is to provide assurance to Government that the state of security within the civil nuclear industry is in line with their expectations. This is achieved, inter alia, through publication of the Chief Nuclear Inspector's Annual Assurance Report, which provides an overview of the safety and security of the UK nuclear, regulated estate. It presents data relating to regulatory activity, events and issues, together with a supporting narrative. It also provides evidence and an explanation that supports the safety and security judgements attributed to the regulated sites.
- 2.2 This TAG contains guidance to help ONR Security Inspectors exercise their regulatory judgement. It provides general advice and guidance on how the adequacy of a dutyholder's security performance should be assessed using analysis of data-based metrics and other evidence to justify the security judgements detailed in Government assurance reporting, including the Annual Assurance Report. It does not set out how ONR regulates a dutyholder's performance, or provide examples of the detailed site specific information that is used to make an assessment, such as thresholds for individual metrics and data.
- 2.3 Dutyholders should develop and maintain their own Security Performance Indicators (SyPIs) in line with a common framework that has been developed for industry use. The primary function of these SyPIs is to inform dutyholders of their premises' performance in support of their own assurance processes, in order to drive behaviour and shape their corporate security strategy. These metrics should be made available to ONR CNS and will influence an inspector's judgement. However, because they are primarily designed to meet a dutyholder's assurance requirements, additional metrics or an alternative analysis of data may be required in order to accurately reflect the regulatory perspective.
- 2.4 As this guide will be used by ONR Security Inspectors when considering the adequacy of a dutyholder's submission, it indicates to dutyholders and other stakeholders the

criteria that ONR use as evidence to assess a site's security performance and assign a level of regulatory priority. It is intended that this guide will influence dutyholder behaviour to focus on the issues that are of regulatory concern.

3. RELATIONSHIP WITH RELEVANT LEGISLATION

- 3.1 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 2013 (Reference 3).
- 3.2 Many of the ONR metrics are measured directly or indirectly against NISR 2003. In particular, where Dutyholders are required to hold a NSSP under Regulation 4, compliance against the arrangements detailed in the NSSP is a fundamental measure of a dutyholder's performance. Similarly, those dutyholders directed by the Secretary of State to adopt standards and procedures for the purpose of safeguarding Sensitive Nuclear Information (SNI) in exercise of Regulations 22(7) (b) and (c) will have their compliance assessed against the HMG Security Policy Framework (SPF) (Reference 5). The reporting of security events or matters under Regulations 10, 18 and 22 also informs a dutyholder's metrics and their internal assurance processes.

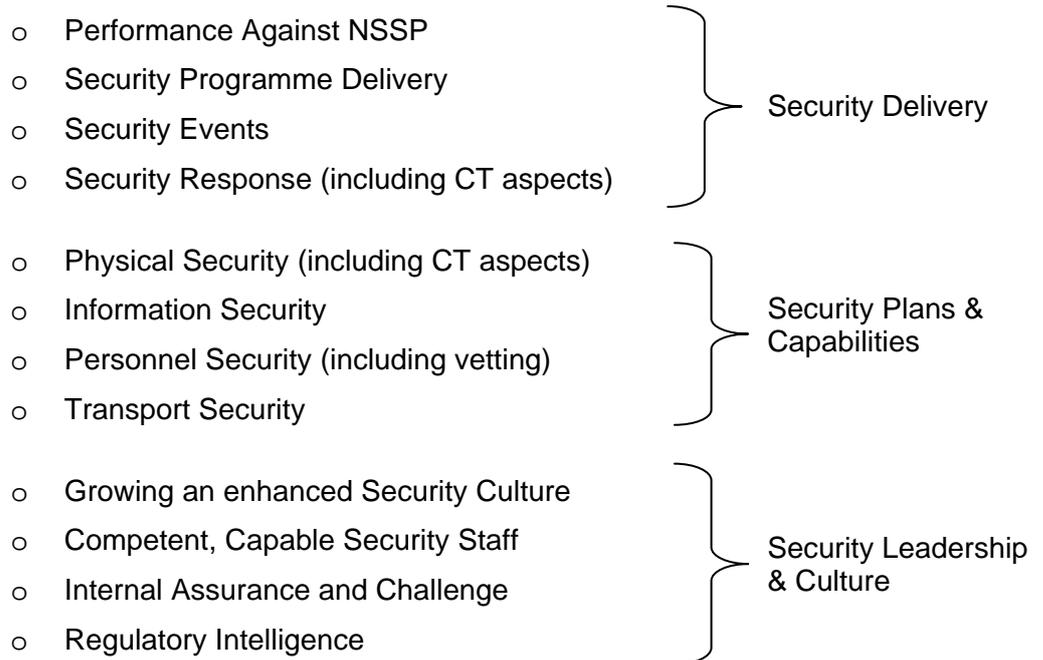
4. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

- 4.1 Dutyholders are required to demonstrate how they meet the security objectives detailed in NORMS through setting out their arrangements and procedures in an approved NSSP. As security regulation progresses towards being an objective focused regime, the requirement for dutyholders to have transparent and robust assurance processes in place will increase. The next iteration of NORMS will include assurance objectives and requirements, which dutyholders will be required to demonstrate are achieved in their NSSP. Where dutyholders' assurance regimes are judged not to fully meet the security objective or are inadequately transparent, ONR inspectors will conduct additional interventions to collect and verify the additional evidence required to form a view of a site's security performance. This may involve inspection activity against a range of site functions that can be mapped across the themes detailed below.
- 4.2 Dutyholders are also required, either by direction or through incorporation within their NSSPs, to adopt the standards and procedures laid out in the HMG SPF, Civil Nuclear Information Security Standard (Reference 6) and Civil Nuclear Personnel Security Standard (Reference 7). These documents are adopted by the whole of the civil nuclear industry for the protection of SNI and the employment of appropriate personnel

security controls on and off nuclear premises. SNI is ascribed a government security classification in accordance with the NISR 2003 Classification Policy (Reference 8).

5. ADVICE TO INSPECTORS – COLLECTION AND ANALYSIS OF EVIDENCE

5.1 Nominated site inspectors are expected to monitor a dutyholder’s security performance throughout the year. They will utilise a range of metric based indicators held on ONR databases as well as information gained through intervention activity such as inspections. Whilst in many cases, quantitative data is available for assessment, in some cases, particularly aspects concerning security culture, it may be binary or purely qualitative. However, irrespective of whether the data is quantitative or qualitative, the inspector should apply analysis (i.e. determine relevance, identify significant elements, consider in light of other information and interpret to form logical conclusions) to the indicators to form a balanced judgement regarding performance and determine the priority level of regulatory attention to be given to the relevant disciplines. These disciplines are set out below:



OVERALL REGULATORY PRIORITY FOR SECURITY

5.2 The overall regulatory priority for security considers the combined performance in three themes; Security Delivery, Security Plans & Capabilities and Security Leadership and

Culture. The first two themes cover the lagging indicators, which are reactive measures of success or failure. It is here that the majority of quantitative data is available for analysis. Leadership and culture contains leading indicators, which are forward looking and strategic in nature. They are of great importance due to their influence on performance. However, with the exception of information collected using the SeCure Tool¹, data in this theme tends to be binary or qualitative, requiring a greater degree of inspector opinion and judgement.

- 5.3 The themes consist of several subgroups and a description of the types of evidence that will be collected and analysed for each is detailed in the paragraphs below. There is no direct correlation between the ratio of priority levels assigned within the subgroups to the overall site priority assessment. This is to allow inspectors to apply judgement on the respective priority according to site categorisation and characteristics of any potential vulnerabilities or allow other factors to influence the final assessment, such as dutyholder attitude, or whether the situation is improving or worsening. However, it would be difficult to justify an overall regulatory priority level of 3, when all of the subgroups are considered to be Priority 2 or higher. The following definitions apply to Priority Levels, 1, 2 and 3:

3

- **Priority 3, Routine Level of Regulatory Attention** – There is clear evidence of good practice in the security regime and/or the NSSP and any appropriate supporting security documentation (e.g. CT plan, Vulnerability Assessments). Any non-compliance has been minimal and only minor security improvements and/or amendments to the NSSP and supporting security documentation have been required in order to meet legal requirements.

2

- **Priority 2, Enhanced Level of Regulatory Attention** – There is evidence of inconsistent application of good practice in the security regime and/or the NSSP and any appropriate supporting security documentation. Instances of non-compliance are apparent, with security improvements and/or amendments to the NSSP and any appropriate supporting security documentation required in order to meet legal requirements. The need for improvement is recognised but plans may be at an early stage.

¹ The Security Culture Review and Evaluation Tool (SeCure), developed by the Centre for the Protection of National Infrastructure can be used by organisations to shape the direction of security policies and also provides a snapshot about how employees view security in the organisation. Results are presented in graphical format to make them easy to interpret, and suggested actions are provided about improvements that could be made. The SeCuRE 2 software tool is available on CD ROM and can be obtained by emailing enquiries@cpni.gsi.gov.uk.

1

- **Priority 1, Significantly Enhanced Level of Regulatory Attention** – There is little evidence of good practice and indication of poor performance/procedure in the security regime and/or the NSSP and any appropriate supporting security documentation. Areas of non compliance are clear, with substantial improvements to the security regime and/or significant amendments to the NSSP and any appropriate supporting security documentation required in order to meet legal requirements. There is likely to be little prospect of improvement in the short term.

5.4 In addition to providing the overall regulatory priority level for the site together with the rationale, this section should also set out any regulatory priorities for the year ahead. These priorities are likely to focus on areas of poor performance deemed to require enhanced or significantly enhanced levels of regulatory attention and the associated security improvement initiatives. To enable this to be done effectively, it may be appropriate for a causal analysis to be undertaken in order that attention is focused on addressing the problem rather than the symptom. However, other major scheduled projects that affect the security regime of the site, such as replacement of the security management system, may also be included as higher priorities.

SECURITY DELIVERY

Performance against NSSP

5.5 Site inspectors conduct scheduled and no-notice inspections at each site over the reporting period as part of routine business. The frequency of visits is determined by the security category and Vital Area (VA) status of the site and further influenced by previous inspection history and any project milestones that may require inspector intervention. Inspections are conducted against the standards detailed in the approved NSSP. Each inspection report is ascribed a rating according to the level of compliance and any non-compliance is detailed in an intervention report. Each non-compliance or shortcoming is graded according to severity/risk and recorded on an issues management system along with the expected corrective action. By analysing inspection report ratings together with the number and grading of non-compliances identified, in conjunction with any aspects of good practice noted, the inspector can form a view on the overall site performance against the NSSP.

Security Programme Delivery

5.6 As detailed above, any instances of non-compliance, together with expected corrective action and the associated timescale are recorded on an issues management system. This system serves three functions; one, it ensures that all required actions are logged and effectively managed through to closure; two, it provides a fully auditable trail of issues management, thereby assisting ONR's internal assurance; and three, analysis of the data provides information to the inspector on how many actions were closed to schedule, closed after an extension being applied to the original timescale, or are currently overdue. Similarly, other improvement actions may also be detailed within the security improvement schedule of a site's NSSP and inspectors should monitor

progress against any agreed milestones or completion dates. This information provides sound evidence as to the performance of site security programme delivery.

Security Events

- 5.7 All nuclear premises² are required to inform ONR of any event or matter falling within the types specified under Regulation 10 of NISR 2003. Additionally, where a site is also an approved Class A or B approved carrier, it is required to report any event within the types specified under Regulation 18, which relate to incidents involving the transportation of Category I to III nuclear material.
- 5.8 Incidents reported to ONR are graded according to severity and the details recorded on a database. Some events or matters are reported for information only and do not affect the security regime of the site, others may not have resulted from any 'fault' on behalf of the dutyholder. However, certain events or matters are considered preventable, and the inspector should use data such as the frequency and severity of these events to make an assessment of performance. This assessment can also be influenced by trending factors i.e. upwards/downwards or multiple repeat events. However, Inspectors should also consider that an increase in reporting of events or matters may not necessarily be indicative of a worsening security regime. Instead, it may be the result of an improved security culture and internal challenge.

Security Response (including CT aspects)

- 5.9 Security response is an important part of a site's security regime and evidence of its effectiveness can be gathered primarily from compliance inspection activity and performance at CT exercises. Aspects of inspection to consider would include the effectiveness of the security management system (integration of alarms, CCTV and expertise of guard force in its use), communications and expediency of alarm response where testing is carried out. CT exercise performance covers guard force and/or armed response initial actions, familiarity with and implementation of contingency plans.
- 5.10 Each civil licensed nuclear site is required to undertake an annual Counter Terrorism (CT) response exercise³ that is assessed by ONR. CT exercise performance should demonstrate capability in; armed and guard force initial response; integrated command and control; effective interoperability and incident management; and, familiarity with contingency plans by SQEP personnel. The implementation of previously identified actions and any other operator initiated improvements to security arrangements and CT response (e.g. improvements to emergency control centres or communication systems) may also influence an inspector's judgement.
- 5.11 Other areas to consider could also include immediate action taken in response to actual events, such as immediate implementation of compensatory measures on

² As defined by NISR2003 Regulation 2.

³ This may be combined with a safety Level 1 Demonstration Exercise. For lower category sites, it may take the form of a desk top or command post type exercise rather than live play.

failure of security equipment, or the ability to back fill shifts and provide cover in the case of sickness. Analysis of the security event database (for example frequency of breaches of minimum security force staffing levels) could provide useful information in this respect.

SECURITY PLANS AND CAPABILITIES

Physical Security (including CT aspects)

- 5.12 When assessing security plans and capabilities, the security inspector makes a judgment as to the continued effectiveness of the approved security plan and supporting security documentation. This includes an assessment of whether the arrangements described are an accurate reflection of the current position and are adequate to meet the security objectives detailed in NORMS, taking into account (where applicable) the threat postulated in Nuclear Industries Malicious Capabilities (Planning) Assumptions (NIMCA) and any associated Vital Area Identification (VAI) studies and Vulnerability Assessments (VAs). It is essential that VAI studies and VAs are kept up to date and accurately reflect current site operations. This ensures that; adequate protection is in place to prevent the potential for unacceptable radiological consequences or theft of nuclear material; and valuable security resource is not wasted on protecting an inappropriate target.
- 5.13 In order to achieve an effective and coordinated response, CT planning documentation should be cognisant of the above whilst also ensuring that it is aligned and integrated with other emergency preparedness documentation; this may include CNC plans, the site emergency plan, the emergency handbook and other appropriate documentation. Command protocols must be clearly documented, as should the purpose of command centres and emergency response personnel.

Information Security

- 5.14 Dutyholders are subject to specialist information security inspections against the standards detailed in the HMG SPF and the Civil Nuclear Information Security Standard. Each inspection report is ascribed a rating according to the level of compliance and any non-compliance is detailed in an intervention report. Each non-compliance or shortcoming is graded according to severity/risk and recorded on an issues management system along with the expected corrective action. By analysing inspection report ratings together with the number and grading of non-compliances identified, in conjunction with any aspects of good practice noted, the inspector can form a view on the overall information security arrangements at the site.
- 5.15 All networks processing SNI are required to have an approved Risk Management Accreditation Document Set (RMADS), or for stand-alone systems, approved Security Operating Procedures (SyOPs). The currency of these documents and the level of compliance against them are also used as indicators.

- 5.16 Lastly, the security event database records events involving breaches of information security policy or procedure. The frequency, severity and reoccurrence of these events is analysed to influence the final assessment.

Personnel Security (including vetting)

- 5.17 Similarly, to information security, sites are also subject to specialist personnel security inspections. These monitor compliance against the HMG SPF and Civil Nuclear Personnel Security Standard and assess the security clearance process, along with the aftercare procedures and personnel security culture that a site has in place. As above, each non-compliance or shortcoming is graded according to severity/risk and recorded on an issues management system along with the expected corrective action. By analysing inspection report ratings together with the number and grading of non-compliances identified, in conjunction with any aspects of good practice noted, the inspector can form a view on the overall personnel security arrangements at the site.
- 5.18 As with information security, the security event database is also analysed for events concerning personnel security and the information used to form part of the final assessment.

Transport Security

- 5.19 Some sites are also approved carriers. All carriers are required to have a Transport Security Statement (TSS) approved by ONR. Inspectors conduct scheduled inspections, which may include no-notice inspections, of every carrier over the reporting period as part of routine business. These compliance inspections are conducted against the standards detailed in the approved TSS. As for information and personnel security, each inspection report is ascribed a rating according to the level of compliance and any non-compliance is detailed in an intervention report. Each non-compliance or shortcoming is graded according to severity/risk and recorded on an issues management system along with the expected corrective action. By analysing inspection report ratings together with the number and grading of non-compliances identified, in conjunction with any aspects of good practice noted, the inspector can form a view on the overall site performance against the TSS.
- 5.20 Approved Transport Security Plans (TptSPs) are required for movements of Category I and II Nuclear Material (NM). Inspectors conduct reactive inspections, which may include no-notice inspections, against some such movements. These inspections are conducted against the standards detailed in the approved TptSP. As with inspections against the approved TSS, each report is ascribed a rating and any non-compliance is detailed and recorded on an issues management system. Analysis of such factors, as well as the timeliness (no less than one month before the proposed shipment) and quality of submission of the TptSP are used as factors in the assessment.
- 5.21 Additionally, it may also be appropriate for site inspectors to make an assessment of a dutyholder's transport security arrangements even where they are not approved carriers. An example of this would be where frequent on-site movements of Category I to III NM are made. These moves are not undertaken in accordance with an approved

TSS or TptSP and in this instance the site inspector would inspect against the arrangements detailed in the NSSP and, as above, analysis of inspection report ratings together with the number and grading of non-compliances would form part of the assessment.

- 5.22 Lastly, in line with paragraphs 5.7 and 5.8, it is also possible to analyse the security event reporting database for those events pertaining to the transportation of Category I to III NM.

SECURITY LEADERSHIP AND CULTURE

Growing an Enhanced Security Culture

- 5.23 A range of factors, many of which are qualitative, influence the assessment of a site's security culture. Typical examples are the attitude of management at all levels and staff towards security and the drive for continuous improvement. General levels of compliance and analysis of the security event database, particularly with respect to repeat events, allow a more quantitative aspect to be included in the assessment.
- 5.24 Many dutyholders have committed to use the SeCuRE Tool developed by the Centre for the Protection of National Infrastructure (CPNI), which will provide a quantitative assessment of security culture and awareness. It also enables the results to be benchmarked against the civil nuclear and other industries. Where dutyholders have implemented the CPNI SeCuRE Tool programme, it should be considered by inspectors in assessing a range of subgroups across the security Leadership & Culture Theme.

Competent, Capable Security staff

- 5.25 The assessment of this subgroup is informed from a range of aspects based around the site being an intelligent customer for security. For example, what is the quality of submission of NSSPs or Temporary Security Plans (TSPs)? How innovative are the operator derived solutions for security issues? How effective is the response/investigation into security events? What experience and qualifications do security management and guards have? What is the currency of the training provided?
- 5.26 Other areas for consideration include the adequacy of resourcing, which might affect timely submission of TSPs or response to actions. Failure of the security force to maintain minimum staffing levels may also be a factor.

Internal Assurance and Challenge

- 5.27 This assessment is based on the quality and robustness of a site's internal assurance processes. This includes internal inspection programmes and peer review, perhaps involving external contractors to provide additional challenge. Evidence of a robust internal challenge function is provided by the proactive rectification of security issues, leaving fewer to be identified by ONR CNS inspectors during compliance inspections.

- 5.28 As described earlier in this TAG, the industry is currently in the process of developing SyPIs as part of a drive to improve internal assurance processes. These indicators will drive improvements to internal assurance and challenge processes. Where dutyholders have developed a robust, transparent and mature set of SyPIs, inspectors should consider using the evidence and data they provide to assist in their assessment of performance against each of the themes. As with the SeCuRE Tool, SyPIs will be of particular use when making judgements against the Security Leadership & Culture Theme, where quantitative or qualitative evidence is typically more difficult to collect.

Regulatory Intelligence

- 5.29 In this subgroup the inspector looks for evidence of operational experience processes, particularly the swift introduction of effective and robust mitigating action in response to security events and matters. Analysis of the security event database for repeat events and trends provides evidence of the efficacy or otherwise of any such action. Additionally, implementation of learning from exercises is of high importance. The presence of softer methods of delivery such as toolbox talks, safety messages and posters can also contribute towards any assessment.

6. ADVICE TO INSPECTORS – PRODUCTION OF ASSURANCE REPORT

- 6.1 In making assessments and providing assurance statements to Government, it is not appropriate to simply publish raw data because it is of little use without proper analysis. For example, to compare raw data from a large, Category I site such as Sellafield with that of a smaller and less complex site would lead to inappropriate conclusions being drawn. Furthermore, an increase in open security improvement actions may reflect improvements in dutyholder security resource and capability, rather than degradation in delivery against the NSSP. Therefore, in all cases, it is the inspector's interpretation and analysis that forms the content of the performance report rather than the data which underpins it. Furthermore, drawing simple conclusions from data has the impact to drive perverse dutyholder behaviour by reducing transparency or focusing delivery solely on achieving an arbitrary target.
- 6.2 In collecting evidence against themes and subgroups, inspectors are to consult with relevant ONR CNS information, personnel and where appropriate, transport security technical specialists. Once adequate data has been collected against each subgroup, inspectors should tabulate the regulatory priority level assessment against them. Each priority level assessment should be supplemented by relevant data with analysis (such as trending) and qualifying statements. An example of a completed priority table and assurance report is included at Annex 1. Whilst the process of collecting metric data is continual and cumulative throughout the year, the assurance report presents information as a snap shot in time, and inspectors should take this into consideration when making assessments.
- 6.3 In light of the above, Inspectors should keep an open, working copy of the report regularly updated throughout the year with the aim of having the initial draft prepared by the middle of April. This will allow time for the performance report to be subject to

thorough peer review and moderation by the end of April prior to being incorporated into the Chief Nuclear Inspector's Annual Assurance Report. The initial peer review is to be conducted by delivery leads, prior to final review and moderation by career development managers. Additionally, in order to maintain the principles of openness and transparency, inspectors should also discuss the performance report with dutyholders.

- 6.4 There is ongoing work within ONR on improving emergency preparedness capability maps. It is expected that the processes laid out in this TAG will inform security aspects of future capability maps.

7. 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. **National Objectives, Requirements and Model Standards.** April 2014.
Trim Folder 4.4.2.13778.
5. **HMG Security Policy Framework.**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299556/HMG_Security_Policy_Framework_v11.0_doc.pdf
6. **Civil Nuclear Information Security Standard.** Trim folder 4.4.2.10457.
7. **Civil Nuclear Personnel Security Standard.** Trim Folder 4.4.2.10457.
8. **NISR 2003 Classifications Policy.** Trim folder 2.5.178.

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

8. GLOSSARY AND ABBREVIATIONS

CNSS	Civil Nuclear Security Standard
CNS	Civil Nuclear Security
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CT	Counter-Terrorism
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NORMS	National Objectives, Requirements and Model Standards
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
RAG	Red/Amber/Green
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyPI	Security Performance Indicator
TAG	Technical Assessment Guide
TSP	Temporary Security Plan
TptSP	Transport Security Plan
VA	Vulnerability Assessment
VAI	Vital Area Identification

ANNEX 1: EXAMPLE PRIORITY TABLE AND PERFORMANCE ASSESSMENT REPORT**Introduction**

This appendix provides an example of the priority table and explanatory note headings detailing the types of quantitative and qualitative evidence that might be provided in support of the assessment made. The wording is illustrative only and inspectors are expected to include any additional information as appropriate. Being an example, the information below is fictitious and does not relate to the performance of any particular site or dutyholder.

PRIORITY TABLE AND PERFORMANCE ASSESSMENT REPORT FOR XXXXXXXXX

Overall Regulatory Priority for Security		3			
Security Delivery		Security Plans & Capabilities		Security Leadership & Culture	
Performance against SSP	3	Physical Security (including CT Aspects)	2	Growing an enhanced Security Culture	3
Security Programme Delivery	2	Information Security	3	Competent, capable security staff	3
Security Events	3	Personnel Security (including vetting)	3	Internal assurance, and challenge	3
Security Response (including CT response)	3	Transport Security	3	Regulatory Intelligence	3

Issues Management Database

Grade	20XX			20XX			20XX		
	Open	Closed	To Time	Open	Closed	To Time	Open	Closed	To Time
1	1	1	1	0	0	0	0	0	0
2	5	2	2	6	2	2	4	0	0
3	16	10	9	20	15	12	17	8	2
Total	22	13	12	26	17	14	16	8	2

OVERALL REGULATORY PRIORITY FOR SECURITY

- Inspectors overall assessment of regulatory priority for security at the site
- Basis for assessment
- Areas requiring improvement
- Enforcement activity
- ONR intentions

SECURITY DELIVERY

Performance Against NSSP

- Number of routine compliance inspections in period
- General level of compliance
- IIS ratings
- Number of regulatory issues opened in period, mapped against significance rating
- Number of outstanding regulatory issues
- Priority rating.

Security Programme Delivery

- Number of regulatory issues closed
- Number of regulatory issues closed to original timescale
- General duty holder progress in addressing issues good/adequate/slow
- Security improvement schedule delivery
- Priority rating

Security Events

Significance	20XX			20XX			20XX		
	Phys	Info	Pers	Phys	Info	Pers	Phys	Info	Pers
Major	0	0	0	0	0	0	0	0	0
Moderate	1	0	0	0	0	0	0	0	0
Minor	3	0	1	2	0	0	3	1	0
None	0	0	0	0	0	0	0	0	0
Total	4	0	1	2	1	0	3	1	0

- Summary of security events (frequency/severity)
- Trending analysis
- Priority rating

Security Response (including CT aspects)

- Summary of relevant interventions (e.g. exercise performance regarding initial actions, guard force alarm response)
- Outcomes of interventions and any follow up action
- Priority rating

SECURITY PLANS AND CAPABILITIES

Physical Security (including CT aspects)

- Summary of CT exercise
- Outcome of the CT exercise and any follow up action taken

- Fit for purpose supporting security documentation (NSSP, CT Plans, Vital Area Identification, Vulnerability Assessments)
- Priority rating

Information Security

- Summary of relevant interventions (compliance against SPF, RMADS, SyOPs)
- Outcomes of interventions and any follow up action
- Other factors such as information security related events, quality of SPF return
- Priority rating

Personnel Security

- Summary of relevant interventions (e.g. inspections against Personnel Security Standards)
- Outcomes of interventions and any follow up action
- Other factors such as personnel security related events
- Priority rating

Transport Security

- Summary of relevant interventions (e.g. inspections against NSSP for on-site moves, compliance against TSS/TsptSP for approved carriers)
- Outcomes of interventions and any follow up action
- Other factors such as transport security related events
- Priority rating

SECURITY LEADERSHIP AND CULTURE

Growing an Enhanced Security Culture

- Summary of relevant interventions (e.g. inspections on security induction training, general attitude of staff/management)
- Outcomes of interventions and any follow up action
- Use of SeCuRE Tool
- Priority rating

Competent, Capable Security Staff

- Summary of relevant interventions (e.g. inspections on training, qualifications, experience and resourcing of security management and guard force)
- Outcomes of interventions and any follow up action
- Quality of permissioning submissions (e.g. NSSP amendments, Temporary Security Plans or Temporary Security Arrangements)
- Priority rating

This section is work in progress and will be updated when more detail is available from the nuclear professionalism work ongoing with UCLAN and the SDF.

Internal Assurance and Challenge

- Internal Inspection regime and findings
- Maturity of SyPIs and integration with wider assurance processes
- Priority rating

Regulatory Intelligence

- Maturity of operational experience processes
- Swift, effective action taken in response to security events
- Minimal repeat events
- Priority Rating