ONR GUIDE			
SECURITY ORGANISATIONAL CULTURE			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-2.0 Revision 0		
Date Issued:	January 2018	**Review Date:**	January 2021
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	TRIM Folder 4.4.2.20789. (2017/456584)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1 INTRODUCTION

1.1 The Nuclear Industries Security Regulations (NISR) 2003 (Reference 6.1) contains requirements for responsible persons to make certain arrangements including standards and procedures to ensure the security of the nuclear premises, Nuclear Material (NM) or Other Radioactive Material (ORM) stored on the premises, Sensitive Nuclear Information (SNI) and standards and procedures for the transportation of Category I - III NM.

1.2 Regulation 4 of NISR requires there to be an approved security plan for each nuclear premises[1] which details those arrangements for the protection of NM/ORM and SNI, including contingency plans. Regulation 7 places the requirement for the dutyholder to maintain arrangements in accordance with the approved plan. Similarly, transporters of Category I-III quantities of NM are required to detail their security arrangements in an approved Transport Security Statement in accordance with Regulation 16 and Regulation 17 requires them to maintain those arrangements. For the purposes of this guide, the term security plan will be used to refer to both approved documents.

1.3 The Office for Nuclear Regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 6.2) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

1.4 To assist inspectors, ONR produces a suite of guides to assist them in making regulatory judgements and decisions in relation to the adequacy of compliance. This inspection guide is one of the suite of documents provided by ONR for this purpose.

2 PURPOSE AND SCOPE

2.1 Security plans should be structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guide is to facilitate a consistent and effective approach to inspecting compliance with the arrangements described in the plan and detailed in the underpinning documentation concerning FSyP 2 – Organisational Culture.

2.2 The judgements made by the inspector will primarily relate to the efficacy of the implementation of arrangements described in evidence that supports the security plan to ensure that associated arguments are fully substantiated. However, ONR takes a sampling approach to regulation and it is possible that elements of evidence within the plan or underpinning the plan were not subject to assessment as part of the approval process. Therefore, when reviewing or inspecting evidence as part of the intervention, the judgement may relate to the adequacy of the arrangements which support the approved plan. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 The guidance should not be regarded as either comprehensive or mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections.

[1] As defined by Regulation 2 of NISR 2003.

2.4 The guidance provided is split into three main elements:

1) relation to relevant legislation;
2) an overview of the FSyP and associated SyDP;
3) guidance on inspection of arrangements for organisational culture, and their implementation

3 RELATIONSHIP TO RELEVANT LEGISLATION

3.1 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.

4 OVERVIEW OF FUNDAMENTAL SECURITY PRINCIPLE 2: ORGANISATION CULTURE

4.1 As described in the SyAPs, Reference 2, FSyP 2 is concerned with the development and maintenance of an embedded security culture within the dutyholder organisation. It states that “Dutyholders must encourage and embed an organisational culture that recognises and promotes the importance of security”. The qualifying text describes how safety and security culture will coexist within an organisation, and although there may be differences due to the different needs of each discipline, successful organisations foster an approach that integrates safety and security in a mutually supporting manner.

4.2 The associated SyDP 2.1 considers the maintenance of a robust security culture. It notes the role of the Board to ensure the entire organisation recognises that a credible threat exists, that nuclear security is important and the role of the individual in maintaining a robust security culture. The detailed assessment guide associated with SyDP 2.1 is published by ONR as CNS-TAST-GD-2.1 (Reference 6.3).

4.3 SyDP 2.1 notes that dutyholders are expected to communicate security expectations and standards to all employees and that processes and arrangements should be in place to create and sustain a robust security culture across the organisation and its supply chain and contractors.

4.4 SyDP 2.1 also describes how the arrangements for a robust security culture should be reviewed and assessed by an appropriate, independent governance regime. There should also be a process to review and test the security culture of the organisation and to encourage continuous improvement.

4.5 SyDP 2.1 further describes how the organisational culture should be aligned to support business and security priorities. Any conflict between safety and security cultures should be identified and addressed in a prompt manner. Similarly, any competing safety and security requirements should be managed and reconciled through integrated holistic risk management and decision making processes.

4.6 The role of leaders at all levels within the organisation to display behaviours that support and demonstrate a commitment to security culture is also recognised. Leaders should ensure staff can engage in appropriate levels of decision making as well as reporting and challenge.

4.7 The International Atomic Energy Agency (IAEA) publish Implementing Guide NSS No 7 titled ‘Nuclear Security Culture’ (Reference 6.4) which includes the latest goals of the

IAEA nuclear security programme. This guide explains the basic concepts and elements of nuclear security culture and provides recommendations to assist in planning and implementing a programme to improve organisations' security culture. Where considered appropriate, elements of this guidance has been included in this Technical Inspection Guide (TIG).

4.8 The high level Leadership and Management for Safety requirements defined in General Safety Requirements Part 2 (Reference 6.5) recognise the interaction between nuclear safety and security culture and the importance of fostering both in a harmonious manner.

4.9 The nuclear industry Safety Directors Forum has produced a booklet 'Key Attributes of an Excellent Nuclear Security Culture' (Reference 6.6), which contains additional information and guidance.

4.10 The World Institute for Nuclear Security has published best practice guide 1.4 for nuclear security culture (Reference 6.7). This gives guidance on the factors that encourage a strong security culture.

5 GUIDANCE ON INSPECTION OF ORGANISATIONAL CULTURE ARRANGEMENTS AND THEIR IMPLEMENTATION

PHASES – GENERAL

5.1 Detailed information on all the phases is detailed in ONR Guide GD-064 (Reference 6.8).

PLANNING PHASE

5.2 ONR has developed regulatory strategies for dutyholders. This includes conducting a programme of security culture interventions to confirm positive management of nuclear security culture across the industry. For all of the major sites and facilities, an annual Integrated Intervention Strategy (IIS) plan exists which describes how the strategy is realised through a series of planned inspections. For more detail on IIS plans, see ONR Guide GD-059 (Reference 6.9).

5.3 When planning security culture interventions:

- Review the IIS plan to confirm the inspection is on the plan, or if necessary, that the plan is modified to include the planned inspection.
- Determine the scope of the inspection. Thus, are all the elements of this guide going to be considered at a high level, for example for a small organisation, or is one specific element to be inspected in detail to help build an overall picture of a larger dutyholder?
- Determine the topics to be sampled. Do recent events or other information from the security site inspector suggest a specific topic should be subject to detailed inspection?
- Consider involving a specialist in Leadership and Management for Safety/Security from the Human and Organisational Factors (HOF) specialism.
- Consult with the nominated site security inspector (where applicable) to ensure they are fully aware of all inspection activities taking place and can support and

give a regulatory context, potentially grouping similar inspections, for example on a topic or facility basis.

- Identify which ONR inspectors (safety and security), technical advisers and internal regulators will be involved.

PREPARATION PHASE

5.4 Specific activities when preparing security culture interventions inspectors could include the following:

- Review the inspection history for the dutyholder. Previous IRs and the RID should be reviewed to determine if there are legacy concerns or issues outstanding which may provide an indication of the current security culture.
- Review the inputs and outputs from dutyholder annual reporting and the ONR backbrief process to determine if specific topics should be sampled.
- Review event reports since the last security culture intervention to identify those which have, or could have, been identified by the dutyholder as having identified weaknesses in the security culture of the organisation.
- Review relevant guidance, References 4, 5, 6 and 7, in conjunction with relevant good practice, to develop a clear understanding of the compliance standards that are expected. The scope of the inspection should be decided and articulated through the preparation of an appropriate question set. Review the 'Inspectors should consider' questions from the appropriate TAG and this TIG.
- Consider in advance how the planned inspection is proportionate to the size of the dutyholder as well as the maturity and quality of the dutyholder's security culture programme. If an extensive inspection is planned, can it be justified on the basis of information on security culture rating and security performance of the dutyholder?
- Consider seeking certain documents in advance of the inspection, potentially including some of the following
    - Nuclear security policy statement
    - Threat briefing materials used for training and dissemination
    - Event investigation reports where security culture was determined to be a contributing feature – as well as potentially looking at event reports where security culture could have been a contributing cause, but this hasn't been identified by the dutyholder.
    - Copies of management indicators used to measure security culture over a defined period
    - Current nuclear security culture survey report
    - Current nuclear security culture improvement plan
    - Assurance reports on the effectiveness of the culture improvement plan

DELIVERY PHASE - GENERAL

5.5 The arrangements developed by an organisation to create and sustain a robust security culture should contain a number of discrete elements, including:

Board and management-level standards and expectations;

A process for the assessment and measurement of security culture;

A programme to review and improve the measured security culture;

The implementation of an assurance led review and assessment of security culture.

5.6 Guidance on the inspection of the arrangements made by the dutyholders for these elements and their implementation is defined in the following sections.

DELIVERY PHASE - BOARD AND MANAGEMENT-LEVEL STANDARDS AND EXPECTATIONS

5.7 Led by its Board, the organisation should create and publish a nuclear security policy which is widely available and promoted at all levels within the organisation. The policy should explain that security has a high priority and reflects that a credible threat exists and that individuals all have a role to mitigate elements of that threat.

5.8 Leaders and managers in the dutyholder organisation should ensure the nuclear security policy is embedded within the overall management system and that alongside all the other elements of the management system, the security elements are reviewed and updated periodically.

5.9 Leaders and managers in the dutyholder organisation should ensure that the importance of a good security culture is promoted within all elements of the supply chain which could have an impact on overall security performance.

5.10 Leaders and managers at all levels in the organisation should promote and display standards of behaviour which enable staff to engage with them regarding security concerns. They should clearly articulate the standards of security behaviour they expect of their staff, and set out what sanctions can be applied if these standards and expectations are not met.

5.11 Leaders and managers should be briefed on relevant security threats and similarly have briefed their staff regarding credible threats and their role in responding to them. Briefing materials should be developed and recorded and the organisation should ensure they are used consistently and at an appropriate frequency. The delivery of training associated with these briefing materials should be recorded and arrangements should be in place for those staff who could not receive the training face to face to also be engaged and trained.

5.12 Decision making by managers should have a clear and demonstrable security element. Decision making should be delegated to defined roles and individuals that are suitably qualified and experienced, and those post holders should take due account of the ideas and feedback from their staff. The contributions made by staff should be recognised and accounted for clearly and transparently to gain the maximum level of ownership. Where decisions in the interests of security and safety are not fully aligned, the priority assigned to each should be defined and managers should ensure decisions are reached and recorded in a systematic and repeatable manner. Where necessary, decisions should be elevated to higher levels within the organisation and reviewed by an independent assurance function.

5.13 The reporting and investigation of events to support improvement and prevent repetition should be open and transparent. Decisions made as a result of the investigations should be formally captured and disseminated to appropriate parts of the organisation. The expectations for arrangements made under Licence Condition 7 are equally applicable to those for events of a security origin.

5.14 Inspectors should consider the following regarding the arrangements and their implementation:

Does the organisation have a clear and accessible nuclear security policy statement?

Is the nuclear security policy contained within the overall management system and is that management system reviewed and updated periodically?

Do leaders and managers check to ensure that the security culture of supply chain partners meets their standards and expectations?

Does the dutyholder have a clear mechanism to ensure enclave organisations display ‘site-wide’ behaviours and culture? Do tenant organisations and contractors have access to ‘site-wide’ security training and security culture initiatives?

Are briefing materials which define the current threat or response levels and their applicability to the organisation developed and used?

What arrangements are in place for the recording of balanced decisions? Are priorities between security and safety elements clearly defined? Does the decision making process take account of the impact of decisions on the security culture of the organisation?

When events are investigated, do the arrangements ensure security culture is considered as a contributing feature, and is the potential impact of subsequent improvement programmes on security culture considered?

Could the dutyholder have overlooked security culture as a contributing factor towards reported events?

Do the leaders and managers display behaviours which demonstrate their commitment to the nuclear security policy statement? Do they support and accept challenge?

Do all members of staff recognise the nuclear security policy statement and can they explain their role in its implementation?

Are behaviours – by managers or individual staff – which are not in accordance with defined security practices challenged? Are records available to demonstrate the organisation does not tolerate poor behaviours or practices which leave the organisation vulnerable to external threats? Are sanctions clearly defined and, when appropriate, enforced? The inspector should note that this is an area where a poorly judged intervention could be as likely to produce a detrimental as a positive effect, and thus where specialist HOF support could be useful.

Do annual reviews of staff performance include an element looking at security performance and culture?

Do staff have clear access to the relevant threat briefing materials and do they understand their role (and the role of others including site security teams) in responding to this threat?

Are the briefing materials recorded, reviewed and re-used on a periodic basis?

Is training delivered based on the threat briefing materials recorded and checked to ensure all staff receive the relevant aspects?

For operational security decision making, is a decision log maintained and is it accessible to all relevant staff?

Are event reports and investigations completed in a timely manner and are subsequent improvement programmes fully implemented and completed within appropriate timescales?

Do organisations learn from relevant good practice in other high hazard industries?

How do dutyholders ensure that their security culture is not compromised by other stakeholders involved in their business?

DELIVERY PHASE – ASSESSMENT AND MEASUREMENT OF SECURITY CULTURE AND ASSOCIATED IMPROVEMENT PLAN

5.15 The dutyholders' measurement of security culture can be achieved through a range of direct and indirect indicators and measures. For many organisations, and specifically the larger dutyholders, an annual survey of security culture may be appropriate, either as part of an annual safety or wider organisational culture survey, or as an independent survey. Inspectors should test when the last survey was undertaken and the scope and content of the security section of the survey.

5.16 The indicators should be benchmarked against other industries and parts of the Critical National Infrastructure, to ensure good practices are adopted.

5.17 For all dutyholders, other indirect measures of security culture should also be considered. These include security performance measures and their periodic review by management teams. Security practices in the organisation should also be subject to periodic reviews and reviews following specific events or changes in threat levels. Arrangements should describe how the organisation responds to internal and external changes that may necessitate a review of security in addition to the mechanisms by which periodic reviews are initiated. They should also explain how subsequent improvement programmes are developed and implemented.

5.18 Security related information, including threat briefings, should be communicated quickly through the organisation. Similarly, learning from experience (LfE) both on site, and from others, should also be communicated effectively. The inspector should seek confirmation that security based LfE and threat briefings are communicated in a timely manner by the dutyholder.

5.19 Lessons identified from organisational culture surveys, or from LfE, need to be acted on to embed a culture of continuous improvement and to improve long term security culture.

5.20 The organisation should have a clear improvement plan with SMART (specific, measurable, attainable, realistic, timely) actions. The inspector should look for both arrangements to develop and manage an improvement plan and for evidence of delivery of actions arising from the plan.

5.21 Management and governance arrangements for the security culture improvement plan should include milestones and indicators to confirm actions are being delivered and reviewed to ensure the expected improvements are being realised. The improvement plan should also be subject to review by internal assurance and other internal controls to confirm delivery of actions, and to confirm that the deliverables have been effective and will produce measureable improvements.

5.22 Follow up surveys of organisational culture should ensure they address previously identified gaps and shortfalls, and where appropriate, they should use repeatable measurements to ensure the effectiveness of improvement actions.

5.23 Inspectors should consider the following regarding the arrangements and their implementation:

Are suitable arrangements in place for periodic measurement of security culture?

How and when was security culture last measured?

Are indirect measures of security culture also considered by the dutyholder? Are they credible and realistic surrogates for security culture?

Are arrangements in place to review internal and external events and improve security culture should it be necessary?

Do the arrangements for the review of events allow for shortfalls in security culture to be identified as a contributor or root cause?

Are management arrangements in place to confirm delivery of a security culture improvement plan?

Are internal assurance arrangements in place to confirm delivery and effectiveness of a security culture improvement plan?

Does the dutyholder communicate LfE specific to security?

Are threat briefings communicated in a timely manner?

Is there an improvement plan for security culture which is widely known?

Does the improvement plan contain SMART actions? Are the actions prioritised and is the prioritisation system appropriate?

Is there measurable and valid progress against the actions?

Are the outputs from the actions reviewed to ensure they deliver the expected improvements?

Is the next assessment of security culture planned and is it focussed to ensure previously identified weaknesses have been addressed?

DELIVERY PHASE – ASSURANCE OF SECURITY CULTURE

5.24 The dutyholder should assure themself that an active security culture assessment and improvement programme is operating effectively within the organisation.

5.25 The assurance team should have access to all of the management information regarding security culture measurement and improvement. They should also have access to independent measurement and feedback from their interactions with the wider dutyholder organisation and individuals within the organisation.

5.26 The assurance reporting to senior management and the Board should report on both delivery of a security culture improvement programme and its effectiveness. The assurance function should also generate and provide an independent view on the accuracy and effectiveness of the security culture measurement and management processes. The reporting process should include both written and verbal reporting.

5.27 The assurance teams should have access to (if they are not part of) the investigations and follow up activities in the event of security incidents or shortfalls. They should review the outputs from these activities to confirm they are effective and lessons are learned to avoid future shortfalls and events. They should also review the information they obtain from their own inspection, assessment and other assurance activity programme of work, to benchmark against the results from the security culture reviews by the dutyholder managers. This should provide an independent view of the accuracy of the information on security culture that the leaders and managers are using as the basis of their decision making and improvement programme.

5.28 Inspectors should consider the following regarding the arrangements and their implementation:

- Does the assurance team have arrangements for the periodic review and assessment of the security culture measurement and improvement plans? If so, do these arrangements include a clear line of reporting to the management and the Board regarding the effectiveness of the security culture improvement programme?
- Does the assurance team include security culture as one of the areas they report on?
- Do they use their own inspections and assessments to benchmark the management information generated regarding security culture?
- Do the assurance teams follow up improvement actions to confirm they are effective?
- Is the assurance plan of work sufficiently wide ranging to give an objective view of security culture across the organisation?
- For small dutyholders with no independent assurance function, are the internal challenge arrangements delivering an effective review of security culture measurement and improvement activities?

WRITE UP PHASE

5.29 A summary of the Write Up phase is that the inspection is recorded in an Intervention Report in a timely manner, following the detailed guidance in References 8 and 9.

5.30 It is important to develop actions or issues taking full account of their potential impact on the security culture of the dutyholder. The potential for a poorly defined or worded action or issue to generate an outcome which undermines security culture within the dutyholder is higher than for more sharply focussed engineering based inspections. If appropriate, the inspector should consult peers and their line manager as well as

listening to the views of the dutyholders' managers and assurance teams to ensure the action is suitably developed.

6 FURTHER READING

6.1 Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403

6.2 Security Assessment Principles – 2017 Edition, Version 0

6.3 Maintenance of a Robust Security Culture. CNS-TAST-GD-2.1 Revision 0

6.4 IAEA Nuclear Security Series No. 7. Nuclear Security Culture.

6.5 IAEA Safety Standards. General Safety Standards: GSR Part 2: Leadership and Management for Safety.

6.6 Nuclear Industry Safety Directors' Forum. Key Attributes of an Excellent Nuclear Security Culture.

6.7 World Institute for Nuclear Security. Best Practice Guide 1.4 Nuclear Security Culture

6.8 ONR Guide GD-064 – General Inspection Guide

6.9 ONR Guide GD-059 - Guidance for Intervention Planning and Reporting.