| ONR GUIDE | | | |
|---|---|---|---|
| **SECURITY GOVERNANCE AND LEADERSHIP** | | | |
| **Document Type:** | Nuclear Security Technical Assessment Guide | | |
| **Unique Document ID and Revision No:** | CNSS-TAST-GD-1.1 Revision 1 | | |
| **Date Issued:** | March 2020 | **Review Date:** | March 2025 |
| **Approved by:** | Matt Sims | Professional Lead | |
| **Record Reference:** | CM9 Folder 4.4.2.23373. (2019/346014) | | |
| **Revision commentary:** | Fit for Purpose Review of Revision 0 | | |

## TABLE OF CONTENTS

Published 03/20

## 1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

## 2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's governance and leadership arrangements. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

## 3. RELATIONSHIP TO RELEVANT 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.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers leadership and management for security to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

## 4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle F of the CPPNM refers to security culture and states that all organisations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organisation. The importance of issues relating to Governance and Leadership  are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 2: Identification and Definition of Nuclear Security Responsibilities – 3.2 Responsibilities for all authorised persons are clearly identified and defined; and,

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:

  a) Developing, implementing and maintaining appropriate and effective integrated management systems

  b) Demonstrating leadership in nuclear security matters at the highest levels.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2). This document states that all organisations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management’s commitment to provide guidelines to the staff and to set out the organisation’s security objectives. All personnel should be aware of and regularly educated about physical protection.

## 5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements.  This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve SyDP 1.1 – Security Governance and Leadership, in support of FSyP 1 – Leadership and Management for Security.  The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) describes the Cabinet Secretary’s expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises

5.3 The Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

## 6. ADVICE TO INSPECTORS

6.1 Organisational and cultural shortcomings are identified consistently as the underlying causes of major accidents and events around the world. This applies to the nuclear industry and to other sectors regardless of the technology involved or the regulatory regime. The organisational and cultural issues are often complex but a number of common factors have been identified from the event investigations and research studies. These include: ineffective leadership, inadequate management oversight and scrutiny of security; poor decision making and lack of effective challenge; and failure to apply lessons from experience.

6.2 Most nuclear regulators, including ONR, have recognised the need to consider organisational and cultural factors as part of their regulatory activities. There is also recognition of the need for increased focus on Board/Director/Senior Management levels within organisations due to their strong influence on culture and security.

6.3 As detailed above, the SyAPs incorporate an FSyP on Leadership and Management for Security (L&MfSy). L&MfSy embraces organisational factors, drawing upon lessons from major accidents and events along with studies into the characteristics of high reliability organisations. L&MFSy principles cover the broad areas of governance and leadership, capable organisation, decision making, learning and assurance processes. In the SyAPs document, for each of these principles there are further details on more specific factors relating to broad topic area. This guidance document is focused on governance and leadership.

### Regulatory Expectations

6.4 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies clear security governance arrangements, a commitment to maintaining security at all times and programmes that support strong security governance and leadership.

| **FSyP 1 - Leadership and Management for Security** | Governance and Leadership | SyDP 1.1 |
|---|---|---|
| Directors, managers and leaders at all levels should focus the organisation on achieving and sustaining high standards of security and on delivering the characteristics of a high reliability organisation. | | |

## 7. NUCLEAR SECURITY GOVERNANCE AND OVERSIGHT

### Governance

7.1 The UK Corporate Governance Code published by the Financial Reporting Council in 2014 (Reference 9) defined corporate governance as:

> *Corporate governance is the system by which companies are directed and controlled. Boards of directors are responsible for the governance of their companies. The shareholders' role in governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place. The responsibilities of the board include setting the company's*

> *strategic aims, providing the leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship. The board's actions are subject to laws, regulations and the shareholders in general meeting.*

7.2 Whilst the UK Corporate Governance Code has more recently been significantly revised the above definition is still regarded as the classic definition of Corporate Governance.

7.3 The UK Corporate Governance Code published in July 2018 (Ref 10) together with the Wates Corporate Governance Principles for Large Private Companies published in December 2019 (Ref. 11) provide guidance to UK companies on the standards of governance expected in the UK and are widely regarded as relevant good practice in Corporate Governance.

7.4 Dutyholder boards should have clear roles and responsibilities, both collectively and individually. They should also be questioning and challenging and effective at holding the senior management to account.

7.5 It is essential that dutyholder boards treat security as an appropriate priority when providing strategic direction and leadership. In order to do this effectively, board members must have access to good quality, current security information regarding threats and risks in addition to any operational performance information generated by the organisation, including metrics. Furthermore, boards must have appropriate membership and competence (either through direct experience or readily accessed subject matter experts) to interpret the security information and use it to validate the efficacy of security programmes.

**Oversight**

7.6 Effective oversight should be facilitated through structured, integrated and diverse means such as self-assessments at facility/department level, internal independent oversight or regulation, robust governance structure, external assessments or peer reviews. The level and rigour applied to this oversight should be implemented using a graded approach.

7.7 Sometimes, oversight of nuclear security is delegated (either explicitly or implicitly) to a dutyholder's security department. However, line management also have responsibilities and department managers should continually monitor and question security performance. Therefore it is beneficial for management to have oversight of security as an integral part of their responsibilities.

7.8 Oversight is dependent on information and performance indicators may be adopted to assist in data collection. However, performance indicators are known to have limitations and, therefore, reports on performance should also include qualitative discussion of trends and issues, supplemented by other sources of information such as feedback from staff, event investigations and assessments/audits.

7.9 Self assessments can be valuable but should be supplemented by a robust internal challenge capability that is independent of the operational line management. Such independent oversight or internal regulation function should be adequately equipped with the skills and resources required to perform its role effectively. Furthermore, it should be valued and supported by senior management, even when it is conveying ‘bad news’. Further information is available in the Independent Oversight Good Practice Guide produced by the cross-industry Internal Oversight Working Group (IOWG) and Published on behalf of the Safety Directors Forum (SDF) (Reference 8).

**Inspectors should consider:**

- Does the board have clearly defined roles and responsibilities?
- Is security treated as a priority when providing strategic direction and leadership?
- Are there mechanisms in place to ensure the board receive current, quality security information on threats and risks?
- Has the board got appropriate membership and competence to assess and act effectively on security information?
- Is oversight facilitated through structured, integrated and diverse means in line with the graded approach?
- Is data collected from a range of sources such as performance indicators, staff feedback, event investigations, independent and self-assessment?
- Is there an independent oversight or internal regulation function with the capability, capacity and authority to perform its role effectively?

## 8. NUCLEAR SECURITY LEADERSHIP

8.1 All dutyholders should develop a Nuclear Security Policy (NSyP). The NSyP should be clear, concise and focused on nuclear security. It is an essential document that influences the behaviours, actions and decisions of the board, leaders and managers. Accordingly, its existence and purpose should be communicated and understood across the dutyholder’s managers, staff and contractors. In that regard, TAGs 4.2 and 4.3 provide additional information on management of the nuclear supply chain. They recommend that potential suppliers be subjected to a screening process designed to ensure that they have a positive security culture, which will enable adherence to the NSyP.

8.2 Security plans should reference the dutyholder’s management of the NSyP and commitment to maintain security at all times, ensuring that expectations are met in all situations (adhering to the values and expectations set out in the NSyP is particularly important in high pressure situations – although it is in these instances when there is greater risk of non-adherence). This will help in developing a culture throughout the organisation that is resistant to nuclear security being compromised for cost, programme or other reasons without due cause, consideration and governance.

8.3 Dutyholders should ensure that roles, accountabilities, standards and expectations of behaviour for nuclear security are clear, linked to the NSyP and apply to all from the board down. Communication is essential and the standards and expectations should form an integral part of induction and training programmes (including leadership selection/development and key contractors).

8.4 It is important that everyone adheres to the standards and expectations and therefore compliance should be monitored and reinforced. The lessons from major events world-wide show that inappropriate attitudes and behaviours at the highest levels of organisations can undermine safety or security. Often, senior managers are involved in 'look down' monitoring but a top-level review is missing. Accordingly, dutyholders should demonstrate how assurance is sought that board members and senior/facility managers (in addition to front-line staff) are acting in accordance with the company's standards and expectations.

8.5 Actions demonstrate commitment to nuclear security. The actions and decisions taken by senior management should demonstrate clearly their overriding commitment to maintaining nuclear security. Management should ensure that organisational security arrangements are robust, seek effective solutions to nuclear security issues and set out key objectives and targets for improving nuclear security, with a strong and consistent emphasis on reducing risks. To support these aims, the management team should regularly visit work areas to observe conditions first hand, model and reinforce standards and expectations, and to interact with staff. They should also implement reward systems that promote the identification and management of risk, encourage positive security behaviours and discourage complacency. However, dutyholders should be careful when designing any reward system to avoid it introducing negative drivers and encouraging perverse behaviours.

8.6 Communication and engagement with staff can be a powerful leadership tool. Dutyholders should encourage frequent, face-to-face engagement between Board members, senior management and staff, recording the outcome and seeking improvement where it has been negative. Other interactions such as company news letters should routinely emphasise nuclear security and not be restricted solely to business issues.

8.7 The skills, knowledge and experience of staff should be respected and utilised to inform decision making at senior levels. Dutyholders should therefore also encourage a culture of engagement with staff such that they are genuinely consulted and involved about issues relating to security, rather than simply being informed about decisions that have been taken.

8.8 Good leaders use effective, efficient and dynamic management systems to engender strong, positive security cultures and work processes which drive continually improving security, safety and business performance and ensure on-going compliance with the law. Dutyholders should therefore implement an integrated management system that ensures security is considered in all their activities and is not confined to the quality management system. It also promotes a more consistent approach to treatment of other areas such as environment, safety, transport and safeguards, and other business activities, and reduces the likelihood of incompatible arrangements.

8.9 There are four principles that underpin effective, efficient and dynamic management systems:

**Principle 1 – Ownership and leadership**

The senior management demonstrably own, value and use their management system to achieve their business aims whilst giving due priority to security:

- Through a shared leadership belief that an effective security culture must be underpinned by an effective and efficient management system.
- By advocating adherence to the management system.
- By ensuring that their management system continues to meet current national or international quality management system standards (e.g. as laid out in IAEA General Safety Requirements No GSR Part 2 (Leadership and Management for Safety).
- Developing and deploying effective governance, internal challenge and independent assessment arrangements.

**Principle 2 – Integrated, focused and optimised,**

Senior management understand their changing business requirements and challenges, and proactively develop their management system accordingly.

- The scope of the management system covers all the dutyholder’s activities, from board to shop floor. It should also cover interfaces with external organisations where this is important to security (e.g. supply chain or regulators)
- The extent and detail of management system controls is applied in a proportional manner depending upon risk and complexity of activities.
- The management system integrates all elements of management including security, health, environment, safety, quality, societal and economic elements such that security is never compromised.
- The senior management pursue vigorously all opportunities to improve the effectiveness and efficiency of the management system by:
    - Setting and achieving objectives for continual improvement.
    - Responding and learning from positive and negative events and situations both internally and externally.
    - Establishing effective performance monitoring and feedback mechanisms.
    - Encouraging everyone to contribute improvement suggestions.
    - Critically reviewing performance.
    - Championing improvements

**Principle 3 – Effective processes**

The management system comprises a hierarchy of processes which deliver and support the achievement of business objectives.

- The needs of processes that directly achieve the business aims (e.g.: operations, decommissioning, manufacturing, project management, etc.) determine the scope and extent of support processes (e.g. security plans and design, supply chain management, technical and engineering support, assurance, etc.).

- Process ownership is assigned to suitable senior personnel who have the necessary support, resources and authority to consult, develop, deploy, monitor and improve the processes across all relevant functions.
- Personnel use and value the process arrangements, providing feedback for Improvement.

**Principle 4 – Visible, accessible and used**

The management system is structured such that all personnel:

- Understand the purpose of the management system.
- Know what it looks like, know what their role is and know what parts of the management system apply to them.
- Understand why it is important to comply with instructions and procedures, to report mistakes and make improvement suggestions.
- Can easily access the information relevant to their job.
- The level of detail is pitched at their level of task competency.

**Inspectors should consider:**

- Is there a clear and concise NSyP in place together with commitment to adhere to it?
- Are roles, accountabilities, standards and expectations of behaviour for nuclear security clear, linked to the NSyP and apply to all from the board down?
- Are the NSyP, standards and expectations effectively communicated?
- Does the dutyholder reinforce and monitor compliance with the NSyP, standards and expectations from the board down?
- Does dutyholder management demonstrate clearly their commitment to maintaining nuclear security?
- Does the dutyholder encourage regular face-to-face engagement between the board, the senior management team and staff? (such as visits to work areas to observe conditions first hand, model and reinforce standards and expectations)
- Is there a performance management system in place that promotes nuclear security without inadvertently introducing perverse drivers?
- Are staff routinely consulted and engaged on security issues such that their skills and knowledge are used to inform decision making at senior levels?
- Is there an integrated management system in place that adheres to current relevant good practice?

## 9. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

2. **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.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. (Version 1.1) May 2018 Cabinet Office. https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

6. **NISR 2003 Classification Policy** For the Civil Nuclear Industry Version 8.01November 2017 http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles** – Trim Ref. 2017/121036

8. **Independent Oversight Good Practice Guide.** Produced by the cross-industry Internal Oversight Working Group (IOWG) and Published on behalf of the Safety Directors Forum (SDF). – December 2018: https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/IOWG/SDF_sub-group_Good_Practice_Guide_Issue_2.pdf

9. **The UK Corporate Governance Code.** Financial Reporting Council- September 2014. https://www.frc.org.uk/getattachment/59a5171d-4163-4fb2-9e9d-daefcd7153b5/UK-Corporate-Governance-Code-2014.pdf

10. **UK Corporate Governance Code.** Financial Reporting Council- July 2018. https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code

11. **The Wates Corporate Governance Principles for Large Private Companies** - Financial Reporting Council- December 2018. https://www.frc.org.uk/directors/corporate-governance-and-stewardship/governance-of-large-private-companies

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

## 10. GLOSSARY AND ABBREVIATIONS

| | |
|---|---|
| CPPNM | Convention on the Physical Protection of Nuclear Material |
| CS&IA | Cyber Security and Information Assurance |
| FSyP | Fundamental Security Principle |
| IAEA | International Atomic Energy Agency |
| L&MFSy | Leadership and Management for Security |
| NISR | Nuclear Industries Security Regulations |
| NSS | Nuclear Security Series |
| NSyP | Nuclear Security Policy |
| ONR | Office for Nuclear Regulation |
| SNI | Sensitive Nuclear Information |
| SPF | Security Policy Framework |
| SyAP | Security Assessment Principle |
| SyDP | Security Delivery Principle |
| TAG | Technical Assessment Guide |