ONR GUIDE			
MAINTENANCE OF A ROBUST SECURITY CULTURE			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-2.1 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19072. (2017/100113)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/17

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 arrangements to develop and maintain a strong security culture. 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 security culture 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

security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organisation. The importance of issues relating to security culture is also recognised in the Nuclear Security Fundamentals, specifically Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 c) Developing, fostering and maintaining a nuclear security culture.

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).

4.4 The IAEA also publish Implementing Guide NSS No 7 titled 'Nuclear Security Culture' (Reference 8) which includes the latest goals of the IAEA nuclear security programme. Among these is providing guidance and assistance to help the 'State' establish a strong nuclear security culture to facilitate and optimise human aspects in their national nuclear security programmes. 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 TAG.

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 2.1 – Maintenance of a Robust Security Culture, in support of FSyP 2 – Organisational Culture. 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.

5.4 Whilst it is not a national policy document, the nuclear industry Safety Directors Forum has produced a booklet 'Key Attributes of an Excellent Nuclear Security Culture' (Reference 9), which contains additional information and guidance.

6. ADVICE TO INSPECTORS

6.1 A dutyholder's nuclear security regime takes into account a range of elements and activities. These include the requirements of regulation, consideration of the threat to Nuclear Material (NM) and Other Radioactive Material (ORM), associated locations/facilities, administrative systems, technical hardware systems, response capabilities and mitigation activities. No single government or industry organisation can address all these elements in isolation and an effective nuclear security culture is

dependent on proper planning, training, awareness, operation and maintenance, as well as on the people who plan, operate and maintain nuclear security systems.

6.2 Even a well-designed security system can be degraded if procedures in place to operate and maintain it are inadequate, or if a dutyholder fails to follow sound procedures. Therefore, a dutyholder's nuclear security regime is dependent on the staff involved and their management, and it is the human factor, including management and leadership, that should be addressed in any effort to enhance existing nuclear security culture.

Regulatory Expectation

6.3 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies appropriate measures and a clear commitment to support a strong security culture throughout the organisation, recognising the importance it has in maintaining an effective nuclear security regime.

FSyP 2 - Organisational Culture	Maintenance of a Robust Security Culture	SyDP 2.1
Dutyholders should ensure that the Board gives due priority to the development and maintenance of a security culture necessary to ensure the entire organisation recognises that a credible threat exists, nuclear security is important and the role of the individual in maintaining it is key.		

7. COMPONENTS OF NUCLEAR SECURITY CULTURE

7.1 Nuclear security culture in the UK has three major components. The first concerns the policy that the government requires to be in place given national and international contexts and how this policy is adopted by the dutyholder. The second is the organisation introduced by a dutyholder to apply government policy in this area and the subsequent management of that organisation. The third component concerns the attitude of individuals at all levels in an organisation towards implementing this policy and making it an integral part of their work and responsibilities.

7.2 ONR also has a responsibility to lead by example and engage with a dutyholder regarding any improvement that may be needed in a site's nuclear security culture when necessary, using appropriate regulatory interventions.

8. RELATIONSHIP AND DIFFERENCES BETWEEN NUCLEAR SAFETY CULTURE AND NUCLEAR SECURITY CULTURE

8.1 Nuclear Safety and Security culture are defined as:

- **Nuclear Safety Culture.** 'That assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance'.

- **Nuclear Security Culture.** 'The assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions which serve as a means to support and enhance nuclear security'.

8.2 Nuclear safety primarily considers the risk of inadvertent human error and to a lesser extent deliberate acts that could cause harm, which are referenced in ONR's Safety Assessment Principles for Nuclear Facilities (Reference 10). In contrast, nuclear security places more emphasis on the prevention of malicious capabilities relating to the theft and sabotage of NM and ORM and to a lesser extent on performance failings or inadvertent human error.

8.3 For a safety culture, great emphasis is placed on sharing information openly, because of an overriding concern for transparency and dialogue wherever possible. A strong security culture places responsibility on a dutyholder to respond immediately to confirmed or perceived threats/incidents and to restrict associated communication to authorised persons on a strict 'need-to-know' basis. That does not necessarily preclude the sharing of suitably expurgated case histories where there is value in doing so. Although there is a difference in approach in some areas, both safety and security cultures need to coexist and should wherever possible reinforce the goals of each, because they share a common objective of limiting the risk resulting from non-malicious and malicious acts associated with NM, ORM (including transport) and associated facilities. This objective is founded largely on similar principles. For example, adopting a questioning attitude, rigorous and prudent approaches, and effective and communication.

8.4 It should be noted that a security culture will require different attitudes and behaviour, compared with a safety culture, such as, when appropriate, the confidentiality of information and the approach taken to deter, detect, delay and respond to malicious capabilities. On occasions when there are differences between safety and security needs, any conflict should be identified by a dutyholder as soon as possible without undermining either discipline.

8.5 A good security culture requires commitment at an organisational level, leadership from managers, and the engagement of other personnel as detailed in Sections 9, 10 and 11 of this document.

9. THE ROLE OF A COMPANY/ORGANISATION

9.1 **Introduction.** An important aspect of a good security culture is the role of a company/ organisation in developing and maintaining systems to ensure that effectiveness of an appropriate nuclear security regime on a site is a high priority for staff. The following paragraphs cover various topics that should be considered when assessing on the adequacy of a security culture.

9.2 **Nuclear Security Policy.** A risk driven security programme which takes due consideration of proportionality is a key element of an adequate security culture. It follows that a dutyholder's security plan should contain a nuclear security policy statement that declares a sound commitment to quality and high performance in all nuclear security activities, and makes it clear that security has a high priority, potentially overriding operational demands where necessary. If there is any conflict regarding the relative priorities of safety, security or operations, senior management should be authorised to resolve the conflict taking into account the overall impact of the risk. This policy underpins the management systems that are an integral part of a company/organisation's security culture and it should be communicated to, and understood by, everyone affected. Nuclear security policy statements may vary in both form and content depending on a site's function, complexity and operational needs. An operating company/organisation has full responsibility for nuclear security in all the

activities under its control and its nuclear security policy statement, endorsed by the company/organisation's Board (or equivalent), should be clear and available to all staff.

9.3 **Management Structure and Systems.** An appropriate, independent governance regime, led by the Board, should exist to ensure that an adequate nuclear security culture is in place and maintained by the use of appropriate management systems/ structures. A primary requirement should be setting out the security expectations and standards that need to be met, which should be communicated to all staff. In this context, the dutyholder should define the roles, responsibilities and accountability for each level within the company/organisation and ensure all staff are accountable for complying with all aspects of the site's nuclear security regime, as detailed in the security plan. In addition, management should appoint an individual who is responsible for nuclear security, with sufficient authority, autonomy and resources to implement and oversee all nuclear security activities. There should also be sufficient resilience to ensure continuity. Where appropriate, management should also establish procedures to facilitate the timely resolution of any conflict between nuclear and radiological safety, security and operations. Management systems should also be in place for each security function to define expectations, determine trustworthiness, implement and maintain processes, measure progress, assess compliance, improve performance through learning from experience, and manage change.

9.4 **Resources.** The company/organisation should allocate sufficient financial, technical and human resources to implement assigned security responsibilities. It should also ensure that all security personnel have the necessary qualifications and that these qualifications are maintained by an appropriate training and development programme. Personnel should also have the necessary equipment, adequate work areas, up to date information and other support to effectively discharge their security responsibilities.

9.5 **Review and Improvement.** As part of an adequate security culture, a dutyholder's security plan should cover the requirement for security performance to be monitored at all levels in the company/organisation from Board level to delivery. This should include ensuring that learning and performance processes for security are in place, and that these are subject to continued improvement, where appropriate. Regular reviews of nuclear security practices should also be conducted taking into account lessons learned from both internal and external reviews, security exercises or incidents, and any relevant changes in the threat. In particular, a dutyholder should ensure that any weakness that relates to nuclear security is comprehensively analysed and expeditiously corrected. As appropriate, experience should be shared with other organisations in the civil nuclear sector, and with ONR. The aim should be to establish an expeditious means of communicating security related information, including learning from experience, and maintain close cooperation with others for the exchange of intelligence and data that could impact on the security of NM/ORM (including transport), associated facilities and SNI.

Inspectors should consider:

- Does the dutyholder have a security policy that incorporates a commitment to quality and high performance in all nuclear security activities?
- Are there mechanisms in place to ensure that the policy is communicated to, and understood by personnel at all levels of the organisation?

- Is there an appropriate, independent governance regime, led by the Board, to ensure that a robust nuclear security culture is in place and supported by management systems and structures?
- Are security expectations and standards clearly set out and mechanisms in place to ensure they are communicated and understood by all staff?
- Is there an individual appointed responsible for nuclear security, who has sufficient authority, autonomy and resources to implement and oversee all nuclear security activities?
- Are there procedures in place to facilitate timely identification and resolution of conflict between safety, security, environment and operations?
- Is there sufficient allocation of financial, technical and human resources to implement security responsibilities?
- Do security personnel have the necessary skills, experience and qualifications to perform their role?
- Is security performance monitored across all levels of the organisation?
- Are there regular reviews of security practices that take into account any lessons learned?

10. THE ROLE OF LEADERS AND MANAGERS

10.1 **Introduction.** The human factor is generally a contributor to all nuclear security related activities and incidents. Therefore, leadership and management are vital components in dealing with malicious capabilities, unintentional personnel errors, inadequate organisational procedures/processes and management failures. The following paragraphs cover various topics concerning the role of leaders and managers that should be considered when assessing the adequacy of a security culture.

10.2 **Influencing Security Culture.** A dutyholder's leaders, including Board members (or equivalent) and managers, can influence security culture throughout a company/organisation by their leadership, example and management practices. With sustained effort, and by employing the incentives and disincentives at their disposal, they should establish appropriate patterns of behaviour and even alter the physical environment where necessary, to facilitate a satisfactory security culture. Normally, leaders and senior managers are responsible for defining and revising policies and security objectives, while operational managers are responsible for initiating practices to comply with these objectives. Through their behaviour, leaders and managers should demonstrate their commitment to nuclear security and, in so doing, play an important role in promoting security culture. Leaders and managers should also foster an effective nuclear security culture by ensuring people understand that a credible threat exists and that effective and proportionate nuclear security is of vital importance in countering it.

10.3 **Decision Making.** Another task for leaders and managers is to carefully consider the views of others and to establish a formal decision making mechanism that is well understood and involves all staff (also see Appendix 1, paragraph 2 b (3)). The quality of a decision is improved when the individuals involved are able to contribute their knowledge and ideas, and take 'ownership' for addressing a problem or implementing

the solution. All personnel should be made aware of, and be committed to, nuclear security requirements and best practices. Security technology should be appropriately used and maintained, and security regulations and procedures properly implemented. Leaders and managers should ensure that the skills and authorisations required to perform tasks relating to nuclear security are in place. Leaders and managers should also maintain effective communications with other companies/organisations to consider, as appropriate, the requirements for protecting NM/ORM (including transport), associated facilities and SNI.

10.4 **Training and Development.** Training and professional development are essential in supporting the expected cultural behaviour. At all levels of an organisation, managers should ensure training is conducted to develop skills and provide tools to promote and implement a strong security culture. Managers should ensure that temporary and permanent staff, including contractors and service providers, understand the importance of protecting NM/ORM (including transport), associated facilities and SNI.

10.5 **Motivation.** All leaders, managers and other staff should understand the specific threats to security that they face and their part (appropriate to their role/responsibilities) in managing and mitigating the risks. Leaders and managers have a key role in ensuring staff are appropriately motivated and their role in enhancing nuclear security is recognised and valued. Performance management tools can encourage vigilance, questioning attitudes and personal accountability. Maintaining and improving nuclear security culture needs persistent effort and frequent monitoring, and leaders and managers have a responsibility to ensure that appropriate behaviour is reinforced through constructive feedback. They should also serve as positive role models through their attention and adherence to nuclear security practices.

10.6 **Reporting of Events and Matters.** As part of a good security culture, leaders and managers should encourage personnel to report any event or matter that could affect nuclear security. Whilst this is a legal requirement in accordance with NISR 2003, Regulations 10, 18 and 22, it also enables dutyholders to monitor trends and address any systemic problems. There should be a well-publicised process in place for reporting which should be reviewed from time to time as considered appropriate by the dutyholder. Part of the review should focus on the need to maintain a reporting system that is effective, whilst being simple to use.

10.7 **Improving Performance.** Leaders and managers should seek continual improvement in nuclear security culture and work to prevent complacency from compromising overall security objectives. They should consider all sources of relevant experience, research, technical developments, operational data, and events of security significance, which should be carefully evaluated and used to enhance nuclear security culture as appropriate. For example, leaders and managers should:

- Ensure that experience and events that affect security, including those from other locations, are analysed and appropriate improvements or corrective actions are implemented;
- conduct self-assessments and arrange for independent audits of the management systems for which they are responsible in order to identify and correct weaknesses;
- establish a programme of exercises to test the performance of security systems and associated human factors such as assessment and response;

- analyse patterns and trends arising from known deficiencies and implement corrections;
- observe operational performance to confirm objectives are being met;
- periodically review training programmes, staff nomination and authorisation procedures, working methods, management systems and staff access processes to sensitive locations, such as Vital Areas (Vas) and to SNI; and,
- maintain an awareness of the need for appropriate security procedures, processes and equipment, so staff have the appropriate tools with which to implement security effectively.

Inspectors should consider:

- Do leaders, including Board members, demonstrate their commitment to nuclear security through their behaviours (leading by example) and management practices?
- Does the organisation employ appropriate incentives and disincentives to establish appropriate patterns of behaviour?
- Do leaders and managers ensure that all staff understand that a credible threat exists and that effective and proportionate security is essential in countering it?
- Do leaders and managers carefully consider the views of others within a formal decision-making mechanism that is well-understood and involves all staff?
- Do leaders and managers ensure that training is conducted across all levels of the organisation to develop skills and provide tools to promote and implement a strong security culture?
- Do leaders and managers encourage personnel to report any event or matter that could affect nuclear security?
- Does the organisation seek continual improvement in nuclear security culture and employ programmes designed to prevent complacency?

11. THE ROLE OF OTHER PERSONNEL

11.1 **Introduction**. A key aspect in achieving and maintaining an adequate security culture is engaging with personnel throughout an organisation. An individual understanding of, and commitment to, security management, roles and responsibilities and a commitment to continuous security improvement are all important in achieving an effective nuclear security culture, which should be included, where appropriate, in approved security plans. The following paragraphs cover various topics concerning the role of non-security personnel that should be considered during an assessment on the adequacy of security culture.

11.2 **Accountability.** For a satisfactory security culture, all personnel should be accountable for their behaviour and should be properly motivated to assist in ensuring

effective nuclear security. Personnel should also be expected to conduct themselves in a manner that recognises the circumstances and potential consequences of their behaviour. Thus they should adopt a rigorous and prudent approach to their security responsibilities, with continuous regard for the security of protecting NM/ORM (including transport), associated facilities and SNI.

11.3 **Compliance with Regulations and Procedures.** Another indication that an adequate nuclear security culture exists is the level of compliance with regulations and associated instructions/procedures, and where constant vigilance and a proactive questioning attitude is evident. All personnel should recognise the importance of protecting SNI as part of an effective nuclear security culture, as well as not sharing site access badges and they should also understand the need to avoid divulging any information that has the potential to undermine security. Whilst staff feedback on procedures and processes should be encouraged, it should not undermine culture or constitute an unauthorised workaround that may compromise compliance.

11.4 **Teamwork and Cooperation**. An adequate nuclear security culture also depends upon teamwork and cooperation among all staff involved in security, which will extend beyond the security team itself. Personnel should therefore understand how their particular roles and relationships contribute to maintaining security.

Inspectors should consider:

- Are all personnel accountable for their behaviour and motivated to assist in ensuring effective nuclear security?
- Is there evidence of a culture of compliance with regulations, associated instructions and procedures?
- Do personnel understand how their particular role contributes to maintaining security?

12. OTHER BEHAVIOURAL CHARACTERISTICS

12.1 A satisfactory nuclear security culture has certain behavioural characteristics common amongst leaders, managers and other personnel, which lead to more effective nuclear security. For most of these characteristics there are performance indicators that provide a means of evaluating and assessing whether a nuclear security culture is adequate and these are detailed in Appendix 1 to this guidance.

13. ASSURANCE AND GOVERNANCE

13.1 As part of developing and maintaining a nuclear security culture, the methods used by a company/organisation should be subject to an internal assurance and governance process by Suitably Qualified and Experienced (SQEP) security and operational staff. This is to ensure that the security culture in place is considered appropriate, effective and proportionate. The extent of this process may vary, taking into account site specific considerations. However, it is important that the Board member (or equivalent) with Board responsibility for security is aware of all aspects of the nuclear security culture and has endorsed the approach used for its development and maintenance.

14. 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**. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

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

8. **IAEA Nuclear Security Series No. 7**. Nuclear Security Culture. http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture

9. **Nuclear Industry Safety Directors' Forum**. Key Attributes of an Excellent Nuclear Security Culture. http://www.nuclearinst.com/Publications

10. **ONR Safety Assessment Principles for Nuclear Facilities.** http://www.onr.org.uk/saps/index.htm

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

15. GLOSSARY AND ABBREVIATIONS

BEIS	Department for Business, Energy and Industrial Strategy
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
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide

APPENDIX 1 - CHARACTERISTICS OF AN EFFECTIVE NUCLEAR SECURITY CULTURE

1. **Introduction**. A company/organisation should provide an assurance that its security regime(s) will accomplish the relevant outcome to detect, delay and respond to any attempted theft, sabotage and other malicious capabilities that threaten the security of NM, ORM, VAs and SNI, whether in use, storage or transport.

2. **Aim**. The characteristics below should be used to supplement the guidance contained in the main body of this guide, which assists ONR security inspectors when assessing the adequacy of a nuclear security culture. It should be noted that the topics covered throughout this guidance are not intended to be viewed as a complete list, or that the topics are applicable in all circumstances. This guidance is primarily aimed at providing examples that can be expanded upon as required, rather than an all-embracing and prescriptive check list. An adequate nuclear security culture should therefore include the following characteristics, which should be detailed as appropriate, in approved security plans:

a. **Management systems**. Staff performance is influenced by the quality of management and provision of expectations, requirements and standards for the conduct of work, training, documented procedures, information systems, etc. Therefore, a well-developed management system is an essential feature of effective nuclear security. The system should prioritise security and include the following topics:

(1) **Security policy**. A nuclear security policy should be developed and made available to all staff. This should indicate that the security function is respected within the company/organisation as a whole. It should refer to a staff code of conduct that includes the needs of nuclear security with which staff are familiar through ongoing training and education.

(2) **Clear roles and responsibilities**. A significant element in establishing an effective nuclear security management structure is the clear definition of roles and responsibilities. Members of a company/organisation should have a clear understanding of 'who is responsible for what' in order to achieve the desired results. It is particularly important to review and update responsibilities when organisational change is being planned and executed. Staff should also understand their roles and responsibilities for nuclear security and be encouraged to seek clarification when necessary. Roles and responsibilities should be adequately explained to new personnel at initial briefings, refresher and/or training sessions.

(3) **Performance measurement**. Quantified nuclear security performance measures, with associated goals, are highly beneficial in establishing management expectations and enabling staff to achieve the desired results. A company/ organisation should use benchmarks and targets to understand, achieve and improve performance at all levels. Performance results compared with the targets should also be regularly communicated to staff and action taken when nuclear security performance does not fully match the goals.

(4) **Work environment**. The physical and psychological work environment has an impact on how staff perform and, therefore, comply with the security requirements. The work environment should be conducive to high standards of performance and staff should be consulted about ergonomics and the effectiveness of their work environment. The text contained in security

instructions and procedures should be easily understood by all staff and the documents themselves should be straightforward to use. Senior site managers should periodically visit security staff to discuss related issues and demonstrate their interest and support.

(5) **Training and qualifications**. An effective nuclear security culture depends on staff having the necessary knowledge and skills to perform their functions to the necessary standard. Consequently, a systematic approach to training and qualification should be in place, which is supported by a comprehensive training programme with agreed requirements and qualification standards that are documented and communicated to staff. Training should be given a high priority and should not be disrupted by non-urgent activities. Periodic evaluations of training programmes should be conducted and revisions incorporated as necessary. Information about the status of staff qualifications should be easily accessed by those who need to know and staff should not be expected to perform work for which they are not SQEP. Where applicable, appropriate, physical fitness criteria should be established and monitored.

(6) **Work management**. All work should be planned to ensure that nuclear security is not compromised and the integrity of the security system is maintained effectively at all times. Contingency plans should be provided for foreseeable events and staff should follow the established plans, or seek prior approval before deviating from planned duties and activities. Work should also be planned in sufficient detail to allow staff to work effectively and efficiently (i.e. resources should be matched to demands).

(7) **Information security**. Protecting SNI is a vital part of the security function and the company/organisation should ensure that requirements are clearly documented in the security plan (and associated instructions) and are well understood by staff. Clear and effective processes and protocols should exist for applying protective markings and safeguarding SNI, inside and outside the company/ organisation. Staff should be aware and understand the importance of adhering to the controls on SNI, including that held or processed on cyber systems, which should be maintained to ensure that they are secure and are operated in accordance with approved procedures.

(8) **Operation and maintenance**. A variety of security systems can be used to achieve nuclear security objectives. For example, those used for accounting, control, physical protection and computer management systems. Nuclear security system equipment will require periodic maintenance and occasional modification and replacement to maintain operations. Operation and maintenance should be performed according to approved procedures and vendor schedules to ensure that design specifications/requirements are not compromised. Checklists/detailed procedures documents can also be used as aids. Compensatory measures should be applied when security equipment is taken out of service for maintenance, when a breakdown occurs, or if it is inoperable for any reason.

(9) **Workforce Trustworthiness**. Any security barrier or procedure can be undermined by an insider or with insider assistance and effective processes to determine trustworthiness and mitigate the insider threat should be in place. Workforce trustworthiness should be conducted, as appropriate, on a regular and ongoing basis. The process for determining trustworthiness should be

capable of identifying specific security risk factors, such as mental illness, drug/alcohol abuse and financial problems. Workforce trustworthiness processes should be rigorously followed and subject to oversight and auditing. These are required for, and should be applied to, all levels of the company/organisation, including temporary staff, contractors, consultants and visitors. Real or apparent failures of workforce trustworthiness processes should be appropriately investigated and remedial action taken as necessary. Training should also be provided to management and other appropriate staff (e.g. HR and Occupational Health) to guide them in identifying apparent high risk behavioural symptoms. Workforce trustworthiness should also address factors that might lead to adverse impacts on reliability and integrity such as substance abuse, workplace violence or criminal and aberrant behaviour.

(10) **Quality assurance**. The security function of a company/organisation requires at least the same degree of rigour, control and assessment as any other major programme area. Therefore, standard quality management practices should be applied. Documented evidence of the benefits of quality management initiatives can convince security personnel that this will assist in gaining trust and support for the organisation and its staff. Assessment processes should be in place for the security function and staff should understand that the management system is of value to the security function and to maintaining specific nuclear security systems.

(11) **Change management**. Problems and failures can arise from an inadequate change management process. This can be true of changes in equipment, procedures, organisational structures and roles or personnel. Therefore, the company/organisation should have effective processes in place to understand, plan, implement and reinforce change as it affects the security regime. Change management processes should also be in place for changes that could affect the security function, whether directly or indirectly, and changes in such areas as operations, safety and security should be coordinated with all potentially affected departments. Any changes should be assessed to confirm that the desired outcomes have been achieved and an evaluation carried out once the change process is complete to see if the change has affected any established security procedures.

(12) **Feedback process**. A company/organisation should learn from its own experiences and the experience of others where possible, so it can continuously improve its nuclear security performance. To do this effectively, processes should exist for obtaining, reviewing and applying experience from internal and external sources. These processes should also obtain, review and apply the available national and international information that relates to security and nuclear security function. Processes should also be in place to allow and encourage staff, contractors and members of the public to report abnormal conditions, concerns, actual events or near misses. Where appropriate, those who report such things should be adequately rewarded and they should be given feedback on action taken by the dutyholder. All such reports should be reviewed by management together with the corresponding action taken to ensure that the company/organisation learns from experience to improve its performance.

(13) **Contingency plans and security exercises**. The nuclear security system should be able to handle any security event without notice. Thus,

contingency plans should be in place to deal with attempted or successful malicious acts, the failure of a security system, or a breach of security. Appropriate and realistic security exercises should be conducted to test and practice these contingency plans. Doing so will confirm the plans are effective and current, and that the individuals involved understand the plans and their roles. All security systems should be tested periodically to ensure that they are functional and available when needed. Special attention should also be paid to systems that are not activated during normal operation. Human factors impacting on security systems should also be evaluated periodically to ensure that personnel are alert, available when needed, and can effectively respond to an incident. Special attention should also be paid to ensuring this during periods of reduced activity, such as Bank Holidays and at weekends.

(14) **Self-assessment**. A company/organisation should have/develop a self-assessment process to confirm it has an adequate security culture. Depending on the complexity of the site, this could include a range of assessment programmes, including root cause analysis, performance indicators, lessons learned and a corrective action tracking programme. Identified deficiencies should be analysed to identify and correct emerging patterns. Performance should also be benchmarked to compare operations against national good practices and operational performance should be observed to confirm that expectations are being met. Corrective action plans should be developed on the basis of self-assessment findings and implementation of these should be monitored.

(15) **Interface with ONR and Government**. Effective nuclear security involves a constructive working relationship between various stakeholders. It is important, therefore, to ensure that information is exchanged regarding important nuclear security matters. The relationship is not only that between ONR and the company/organisation, but also with others, such as BEIS, CPNI and NCSC. Information regarding vulnerabilities and threats should be communicated in a timely manner following relevant protocols.

(16) **Coordination with off-site organisations**. Staff and management in organisations/companies should establish lines of communication with relevant local and national organisations that support nuclear security. If necessary, written agreements/Memoranda of Understanding (MoU) should be in place with appropriate organisations, such as Home Office police forces and Police Scotland, to facilitate assistance, communication and timely response to incidents.

b. **Behaviour that fosters a more effective nuclear security**. Leaders and managers are responsible for ensuring that appropriate standards of behaviour and performance for security are set and expectations for applying these are understood. They should ensure there is a clear understanding within a company/organisation of the security roles and responsibilities of each individual, including clear statements on levels of authority and lines of communication. Behaviour is an observable action or statement. Individuals are inclined to learn and imitate the prevailing patterns of behaviour that exist in the group around them, and once established these patterns can be difficult to alter. The effectiveness of nuclear security depends on the correct behaviour of all personnel, including their vigilance, challenge and completing work as planned. The following should be taken into account:

Leadership behaviour

(1) **Expectations**. Leaders should establish and clearly communicate their performance expectations for nuclear security. Doing so will assist staff in meeting their responsibilities in support of the nuclear security regime. Leaders should ensure that there is sufficient resource to support an effective nuclear security regime. They should lead by example and, as is expected from all staff, adhere to the extant security policies and procedures. Leaders should personally assess performance by conducting walk-throughs, listening to staff and observing work being carried out and be able to identify any weakness in the extant security situation. They should take appropriate action to correct any deficiencies they note. Significant security vulnerabilities should be rectified as a priority.

(2) **Use of authority**. Leaders should establish the responsibility and authority for each role within the security organisation which should be clearly and properly documented. Leaders should be able to demonstrate a sound understanding of what is expected of them, and recognise and take charge should a security problem occur, particularly if it increases vulnerability (e.g. when the security system is degraded or the threat level is raised). They should be approachable and encourage effective communication so staff will readily report their concerns. Finally, leaders should not abuse their authority by circumventing security.

(3) **Decision making**. Decisions should be made by those SQEP and authorised to do so. Leaders are expected to make decisions when the situation warrants it and explain/justify their decisions as necessary. The process through which a company/organisation makes decisions is an important part of nuclear security culture. Adherence to formal and inclusive decision making processes can demonstrate the significance that management places on the making of security decisions, and help improve the quality of these decisions. Leaders should take account of dissenting views and different perspectives, to improve the quality of the decisions made. They should not shorten or bypass decision-making processes.

(4) **Management oversight**. An effective nuclear security culture is dependent on individuals' behaviour and this is strongly influenced by people's supervisory skills. Therefore, leaders and their managers should spend time observing, correcting and reinforcing the performance of staff at work and use constructive feedback as a means of reinforcing the behaviour expected from staff. All staff should be accountable for conforming to established security policies and procedures.

Staff behaviour

(1) **Involvement of staff**. Security performance can be improved when staff are able to contribute their ideas and mechanisms should be in place to support their doing so. Where possible, leaders and managers should involve staff members in risk assessment and decision-making processes. Staff should be encouraged to make suggestions and be properly recognised for their contributions.

(2) **Effective communications**. An important part of an effective nuclear security culture is to encourage and maintain the flow of official information throughout the company/organisation, ensuring that communication is valued and that any potential blockages in communication channels are addressed. Communications should be used to explain the context for issues and decisions where possible, by visiting staff at work and/or holding meetings where staff can ask questions. Staff input should be welcomed and where appropriate staff should be kept informed on high level policy and organisational changes.

(3) **Improving performance**. A company/organisation should aim for continual improvement in nuclear security performance. Leaders and managers should establish processes and show by personal example and direction, what they expect staff to do. Staff should be encouraged to report problems and make suggestions for improving the nuclear security regime. The causes of events and matters should be identified and corrected. An internal process should also exist for staff to raise nuclear security concerns directly with their immediate supervisors, senior managers or leaders.

(4) **Motivation**. Staff motivation and attitudes affects behaviour. Motivating individuals and groups will help improve the effectiveness of a nuclear security regime. Leaders and managers should encourage, recognise and reward commendable attitudes and behaviour and help counter the insider threat by stressing to individuals their responsibility for watching for, and reporting unusual occurrences. Where appropriate, performance management systems should recognise staff contributions in maintaining an effective nuclear security culture, and staff should be aware of the system of rewards and sanctions that relate to nuclear security. Annual performance appraisals should include a section on nuclear security performance. When applying disciplinary measures in the event of violations, sanctions for self-reported violations should, where possible, be tempered to encourage the reporting of future infractions.

Behaviour of all Personnel (Leaders, Managers, Staff)

(1) **Professional conduct**. An important aspect of nuclear security culture is a company/organisation's expectation that all personnel are professional in their approach to nuclear security. Personnel should be familiar with the company/organisation code of conduct. They should adhere to it and take pride in their work, assisting others where necessary and interacting with professional courtesy and respect.

(2) **Personal accountability**. Accountable behaviour means that all personnel understand their specific tasks in relation to nuclear security (i.e. what they have to accomplish, by when, and what objectives should be achieved) and they complete these tasks as expected, or report their inability to do so to their supervisor. Behaviour that enhances security culture should be reinforced by leaders and managers and all personnel should take responsibility, where appropriate, to resolve security issues.

(3) **Compliance with security plans**. Requirements detailed in security plans should be met and any supporting security procedures and instructions adhered to. It is important, therefore, that all security instructions and procedures are clear, up to date, readily available, and user friendly, so personnel will not deviate from approved methods due to a lack of clarity.

(4) **Teamwork and cooperation**. Teamwork is essential, and an effective nuclear security culture can best be formed in a company/organisation where there is sound and extensive interpersonal cooperation/interaction, and where relationships are generally positive and professional. Teams should be recognised for their contribution to nuclear security and personnel should be encouraged to interact with openness and trust and be seen to routinely support each other.

(5) **Vigilance**. Good security can depend on the vigilance and observational skills of personnel, and the prompt identification of potential vulnerabilities. Personnel should be encouraged to take notice of and question unusual behaviours and events, and report them to management as soon as possible. Personnel should also be encouraged to seek guidance when unsure of the security significance of unusual events, observations or occurrences.

c. **Some Fundamental Principles for guiding decisions and behaviour**.

(1) **Motivation**. Behaviour is dependent upon the strength of beliefs, values and performance of personnel. Leaders and senior managers should encourage, reinforce and support these to ensure staff are well-motivated and share a common purpose.

(2) **Leadership**. Fundamental influences on individual performance are the expectations of leaders. Nuclear security is most effective when leaders, managers and staff continually demonstrate their commitment to security through their words and actions.

(3) **Commitment and responsibility**. Nuclear security is most effective when all personnel (leaders, managers and staff) take personal responsibility for maintaining the extant security regime.

(4) **Professionalism and competence**. Effective nuclear security requires personnel to have the right qualifications, skills and knowledge they need to perform all aspects of their work. Appropriately qualified and trained personnel should also be able to respond effectively to all contingencies and emergencies.

(5) **Learning and improvement**. Nuclear security can be improved by continual self-assessment, understanding why mistakes occur, and dealing effectively with the lessons learned.