



ONR GUIDE			
GUIDANCE ON THE ASSESSMENT OF NUCLEAR SECURITY CULTURE WITHIN DUTYHOLDER ORGANISATIONS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-002 Revision 1		
Date Issued:	April 2016	Review Date:	April 2019
Approved by:	Angus Cameron	Superintending Inspector	
Record Reference:	TRIM Folder 1.9.3.936. Unique Ref: 2016/0168148		
Revision commentary:	Document rebranded and minor content updates		

TABLE OF CONTENTS

1. INTRODUCTION.....	2
2. PURPOSE AND SCOPE	2
3. COMPONENTS OF NUCLEAR SECURITY CULTURE	2
4. RELATIONSHIP WITH RELEVANT LEGISLATION	3
5. RELATIONSHIP TO IAEA DOCUMENTS	3
6. RELATIONSHIP WITH NATIONAL POLICY/GUIDANCE DOCUMENTS	3
7. RELATIONSHIP AND DIFFERENCES BETWEEN NUCLEAR SAFETY CULTURE AND NUCLEAR SECURITY CULTURE	4
8. THE ROLE OF A COMPANY/ORGANISATION	4
9. THE ROLE OF LEADERS AND MANAGERS	6
10. THE ROLE OF OTHER PERSONNEL	7
11. OTHER BEHAVIOURAL CHARACTERISTICS	8
12. ADVICE TO SECURITY INSPECTORS	8
13. ASSURANCE AND GOVERNANCE.....	8
14. REFERENCES.....	9
15. GLOSSARY AND ABBREVIATIONS.....	10
16. APPENDIX 1 - CHARACTERISTICS OF AN EFFECTIVE NUCLEAR SECURITY CULTURE.....	11

© Office for Nuclear Regulation, 2016

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

OFFICIAL

OFFICIAL

1. INTRODUCTION

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

2. PURPOSE AND SCOPE

- 1.3. The purpose of this TAG is to advise and inform ONR Security Inspectors in the exercise of their regulatory judgement. It also aims to provide general advice and guidance to ONR staff on assessing the adequacy of nuclear security culture within a company or organisation, as part of the Civil Nuclear Industry. It does not set out how ONR regulates these arrangements.
- 1.4. 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.
- 1.5. 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 must be addressed in any effort to enhance existing nuclear security culture.
- 1.6. This guide is to be used by ONR Security Inspectors to assess the adequacy of a company/organisation's nuclear security culture. It will influence the issues that should be assessed when considering the security culture of an organisation both in practice and as it is described in a NSSP, as detailed in a separate TAG (see CNS-TAST-GD-001). This guide does not prescribe the actual content or detail that needs to be addressed on security culture; this remains the responsibility of the dutyholder. However, it does indicate to dutyholders and other stakeholders the main topics to be considered during the assessment to assist in determining the adequacy of security culture on a site.

3. COMPONENTS OF NUCLEAR SECURITY CULTURE

- 1.7. 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 Regulator (ONR) also has a responsibility to lead by example and engage with a dutyholder regarding any improvement that may be required in a site's nuclear security culture when necessary, using appropriate regulatory interventions. The second is the organisation introduced by a dutyholder to apply government policy in this area. 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. (See Sections **Error! Reference source not found.** and **Error! Reference source not found.**).

OFFICIAL

OFFICIAL**4. RELATIONSHIP WITH RELEVANT LEGISLATION**

- 1.8. The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil licensed nuclear sites and other (unlicensed) nuclear premises subject to regulation, as defined in the Nuclear Industries Security Regulations (NISR) 2003 (References 1 and 2). It is also used to refer to a 'licensee' as defined in paragraph 1 of a Nuclear Site Licence granted under the provisions of the Nuclear Installations Act 1965, or a 'developer' carrying out work on a nuclear construction site, as described in the Nuclear Industries Security (Amendment) Regulations 2013 (Reference 3).
- 1.9. The NISR 2003 (as amended) defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It is a requirement that all NSSPs are to include a section describing the manner in which the site promotes and maintains a nuclear security culture.

5. RELATIONSHIP TO IAEA DOCUMENTS

- 1.10. International Atomic Energy Agency (IAEA) document titled 'Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities' (INFCIRC225 Revision 5 - Reference 4), contains principles that the UK is obligated to take into account. Part 3 of this document refers to the need for all organisations involved in implementing physical protection to give due priority to security culture, its development and maintenance necessary to ensure its effective implementation in the entire organisation. It also mentions that the 'State' should promote a nuclear security culture, encourage all security organisations to establish and maintain one, and that a nuclear security culture should be pervasive in all elements of the physical protection regime.
- 1.11. IAEA Implementing Guide (Ref: NSS No 7) titled 'Nuclear Security Culture' (Reference 5) 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.

6. RELATIONSHIP WITH NATIONAL POLICY/GUIDANCE DOCUMENTS

- 1.12. For the purposes of this TAG the 'license holders' are dutyholders, the 'security plan' is the NSSP, and the 'competent authority' is ONR.
- 1.13. The 'threat assessment/design basis threat' is detailed in the extant version of the Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) document (Reference 6). This document refers to the malicious capabilities, including those associated with the theft and sabotage of nuclear material (NM) and other radioactive material (ORM) that need to be addressed.
- 1.14. Part One, Chapter 1, paragraphs I.1.38, 1.1.39 and Annex D of the NORMS document (Reference 7) covers the requirement for a dutyholder to maintain an effective security culture.
- 1.15. The HMG Security Policy Framework (SPF) is adopted by the whole of the civil nuclear industry for the protection of Sensitive Nuclear Information (SNI) and the employment of appropriate personnel security controls on and off nuclear premises.
- 1.16. NISR Classification Policy (Reference 9) indicates those categories of SNI that require protection and the level of protective marking to be applied.

OFFICIAL

OFFICIAL

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

1.17. 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'.

1.18. Nuclear safety primarily considers the risk of inadvertent human error and to a lesser extent other deliberate acts that could cause harm, which are referenced in ONR's Safety Assessment Principles (SAPs). 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 inadvertent human error. Security requirements are also primarily concerned with countering specific malicious capabilities associated with Category I sites and sites containing High Consequence Vital Areas (HCVAs) and to other Category II to IV sites and sites containing Low and Medium Consequence VAs, (see separate TAGs CNS-TAST-GD-005 and CNS-TAST-GD-006).

1.19. 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. 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 by limiting the risk resulting from non-malicious and malicious acts associated with NM, ORM and associated facilities. This objective is also largely based on similar principles. For example, of adopting a questioning attitude, rigorous and prudent approaches, and effective and open two way communication.

1.20. 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 efforts to deter, detect, delay and respond to malicious capabilities. On occasions when there are differences between safety and security requirements, any conflict should be identified by a dutyholder as soon as possible. (See Part One, Chapter 1, paragraph 1.1.21 of the NORMS document).

1.21. A good security culture requires commitment at an organisational level, leadership from managers and the engagement of other personnel as detailed in sections **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.**

8. THE ROLE OF A COMPANY/ORGANISATION

1.22. **Introduction.** An important aspect of a good security culture is the role of a company/organisation in developing and maintaining systems to ensure that maintaining 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.

1.23. **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

OFFICIAL

OFFICIAL

dutyholders NSSP (see CNS-TAST-GD-001) should contain a nuclear security policy statement that declares a sound commitment to quality of performance in all nuclear security activities, and makes it clear that security has a high priority, even overriding operational demands where necessary. If there is any conflict regarding the relative priorities of safety, security or operations, senior management must 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 role, complexity and operational needs. An operating company/organisation has full responsibility for nuclear security in all the activities under its jurisdiction and its nuclear security policy statement, which should be endorsed by the company/organisations Board (or equivalent), should be clear and available to all staff.

- 1.24. **Management Structures and Systems.** An appropriate, independent governance regime, led by the Board, should exist (see paragraph 13) to ensure that an adequate nuclear security culture is in place and it is 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 and understood by 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 compliance with all aspects of the site's nuclear security regime, as detailed in the NSSP. In addition, management must 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 the various facility operations. Management systems should also be in place for each security function to define expectations, implement and maintain processes, measure progress, assess compliance, improve performance through learning from experience and manage change.
- 1.25. **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.
- 1.26. **Review and Improvement.** As part of an adequate security culture, a dutyholder's NSSP should cover the requirement for security performance to be monitored at all levels in the company/organisation from Board level to delivery. This process 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 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 industry, and with ONR. The aim should be to establish an expeditious means to communicate security related information, including learning from experience, and maintain close cooperation for the exchange of intelligence and data that could impact on the security of materials and facilities, including transport.
- 1.27. The aspects mentioned in the paragraphs above are an important part in an adequate nuclear security culture and further information on accountabilities and the management of

OFFICIAL

OFFICIAL

security is contained in Part One, Chapter 1, paragraphs 1.1.22 to 1.1.28 of the NORMS document.

9. THE ROLE OF LEADERS AND MANAGERS

- 1.28. **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.
- 1.29. **Influencing Security Culture.** A dutyholder's leaders, including Board members (or equivalent) and managers, can influence security culture throughout a company/organisation through 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 provide an adequate 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.
- 1.30. **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 in the decision making process (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. All personnel must 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 must 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 material and SNI.
- 1.31. **Training and Development.** Training and professional development are essential in supporting the expected cultural behaviour. At all levels of an organisation, managers must 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, together with any external or self-employed service providers, understand the importance of protecting radioactive material and associated facilities, including transport and sensitive information.
- 1.32. **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. Rewards and recognition, both tangible and intangible, can encourage vigilance, questioning attitudes and personal accountability. Maintaining and improving nuclear security culture can require 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.

OFFICIAL

OFFICIAL

- 1.33. **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 requirement in accordance with NISR 2003, Regulations 10, 18 and 22 it also enables dutyholders to monitor trends and address any systemic problems. The process in place for reporting 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.
- 1.34. **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 together with 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 VAs and to SNI; and
 - maintain an awareness of the requirement for appropriate security procedures, processes and equipment, so staff have the appropriate tools with which to implement security effectively.

10. THE ROLE OF OTHER PERSONNEL

- 1.35. **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 covered where appropriate in approved NSSPs. 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.
- 1.36. **Accountability.** For an adequate 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. This requires them adopting a rigorous and prudent approach to their security responsibilities, with continuous regard for the security of NM, ORM, (on site and in transport) other related VAs and SNI.

OFFICIAL

OFFICIAL

- 1.37. **Compliance with Regulations and Procedures.** Another indication that an adequate nuclear security culture exists can be characterised by compliance with regulations and associated instructions/procedures, and where constant vigilance and a proactive questioning attitude is evident by personnel. All personnel should recognise the importance of protecting SNI as part of an effective nuclear security culture and they should also understand the need to avoid divulging any information that has the potential to undermine security.
- 1.38. **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 interfaces contribute to maintaining security.

11. OTHER BEHAVIOURAL CHARACTERISTICS

- 1.39. An adequate 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 guide.

12. ADVICE TO SECURITY INSPECTORS

- 1.40. ONR Security Inspectors should decide whether a security culture within a company/organisation is adequate taking into account the guidance detailed in the above paragraphs and in Appendix 1 to this guide. It should be remembered that assessing the adequacy of a site's nuclear security culture will form part of regulatory activities by Security Inspectors; therefore the extent of a nuclear security culture should also be referred to as appropriate, in a dutyholder's NSSP.

13. ASSURANCE AND GOVERNANCE

- 1.41. 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 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) for security is aware of all aspects of the nuclear security culture in place and has endorsed the approach used for its development and maintenance.

OFFICIAL

OFFICIAL**14. REFERENCES**

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

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

OFFICIAL

15. GLOSSARY AND ABBREVIATIONS

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

OFFICIAL**16. 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 its objectives (as detailed in NORMS) to prevent, detect, delay and respond to any attempted theft, sabotage and other malicious capabilities that threaten the security of NM, ORM, VAs and SNI, 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 guide are not intended to be viewed as a complete list, or that the topics are applicable in all circumstances. The primary aim of all the guidance is to provide a number of 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 NSSPs:

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. All of these systems should be well developed, prioritise security and adequately cover the following topics:

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

(2) **Clear roles and responsibilities.** A significant part of 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 essential 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 NSSP 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

OFFICIAL

OFFICIAL

straightforward to use. Senior site managers should also periodically visit security staff to discuss related issues and show their interest.

(5) **Training and qualifications.** An effective nuclear security culture depends on staff having the necessary knowledge and skills to perform their functions to the required 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 required to perform work for which they lack the required skills and knowledge. 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 (e.g. 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 NSSP (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. It follows that 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, accredited by ONR, 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 can also be used as an aid and compensatory measures must be put in place, when security equipment is taken out of service for maintenance, when a breakdown occurs, or if it is inoperable for any reason.

(9) **Personnel security.** Any security barrier or procedure can be defeated with Insider assistance and effective processes to determine trustworthiness and mitigate the Insider threat should be in place. Screening should be conducted, when appropriate, on a regular basis and the process for determining trustworthiness should be capable of identifying specific security risk factors, such as mental illness, drug/alcohol abuse and financial problems. Screening 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 the screening processes should be appropriately investigated and

OFFICIAL

OFFICIAL

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 and in applying observational and analytical skills. The screening process should also address factors that might lead to degradation of trustworthiness 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 quality service helps gain trust and support for the organisation and the people in it. Assessment processes should be in place for the security function and staff should understand that the management system is relevant to the security function and to maintaining the nuclear security system.

(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 applies to 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 must 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 any action taken by the Duty Holder. All reports should be reviewed by management with actions taken to ensure that the company/organisation learns from experience in order 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 must 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. The human factor in security systems should also be evaluated periodically to ensure that personnel are alert and available when needed and can respond to deal with an incident. Special attention should also be paid to

OFFICIAL

OFFICIAL

the human factor, 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 and 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 best 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 other departments, such as DECC. Information regarding vulnerabilities and threats should be passed in a timely manner and the regulatory interface points should be clearly defined.

(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/Memorandum 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:

OFFICIAL

OFFICIAL

Leadership behaviour

(1) **Expectations.** Leaders should establish and communicate their performance expectations for nuclear security. Doing so will assist staff meet 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 then be clear and properly documented. Leaders should be able to demonstrate a good 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 two way communication so staff will readily report their concerns. Finally, leaders should not abuse their authority to circumvent security.

(3) **Decision making.** Decisions should be made by those qualified and authorised to do so. Leaders are expected to make decisions when the situation warrants and explain or 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 dependant 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 adherence 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 this objective. Where possible, leaders and managers should involve staff members in the 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 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

OFFICIAL

OFFICIAL

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 to continuously improve nuclear security performance. Leaders and managers should establish processes and show by personal example and direction, what they expect staff to consider. Staff should be encouraged to report problems and make suggestions for improving the nuclear security regime. The causes of events and matters (which is covered in a separate TAG Ref: CNS-TAST-GD-011) 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 (see the NORMS document) by stressing to individuals their responsibility to watch for and report unusual occurrences. Where appropriate, reward systems (such as Team or individual bonuses) 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 also 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 the NSSP.** Requirements detailed in NSSPs 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 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.

OFFICIAL

OFFICIAL

(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 indications and occurrences, 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 must encourage, reinforce and support these to ensure staff are well-motivated and share a common purpose.

(2) **Leadership.** The greatest 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 maintaining the extant security regime.

(4) **Professionalism and competence.** Nuclear security requires all personnel to have the 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.

OFFICIAL