ONR GUIDE			
ORGANISATIONAL SECURITY CAPABILITY			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-1.2 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19071. (2017/100002)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1. INTRODUCTION 2
2. PURPOSE AND SCOPE 2
3. RELATIONSHIP TO RELEVANT LEGISLATION 2
4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE 2
5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS 3
6. ADVICE TO INSPECTORS 3
7. REFERENCES 12
8. GLOSSARY AND ABBREVIATIONS 13
APPENDIX 1: PRINCIPLES OF A NUCLEAR BASELINE (NB) 14
APPENDIX 2: MANAGEMENT OF CHANGE PRINCIPLES 15
APPENDIX 3: BROAD GUIDANCE ON CLASSIFICATION OF ORGANISATIONAL CHANGE 16
APPENDIX 4: DESIGN AUTHORITY CAPABILITY PRINCIPLES (DA) 17

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 organisational capability. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

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

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

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

4.2 Fundamental Principle F of the CPPNM refers to security culture and states that all organisations involved in implementing physical protection should give due priority to

the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organisation. The importance of issues relating to Governance and Leadership are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 2: Identification and Definition of Nuclear Security Responsibilities – 3.2 Responsibilities for all authorised persons are clearly identified and defined; and,
- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:

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

  d) Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear responsibilities on a continuing basis using a risk informed approach.

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).

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 1.2 – Organisational Security Capability, in support of FSyP 1 – Leadership and Management for Security. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 7) 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 8) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

Background

6.1 Organisational and cultural shortcomings are identified consistently as the underlying causes of major accidents and events around the world. This applies to the nuclear industry and to other sectors regardless of the technology involved or the regulatory regime. The organisational and cultural issues are often complex but a number of common factors have been identified from the event investigations and research

studies. These include: ineffective leadership, inadequate management oversight and scrutiny of safety; poor decision making and lack of effective challenge; and failure to apply lessons from experience.

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

6.3 A capable organisation should be adequately resourced, ensuring sufficient Suitably Qualified and Experienced Persons (SQEP) are available in sufficient numbers to deliver resilience. It should have the governance structures to ensure the security arrangements are implemented and maintained through demonstrable Leadership and Management for Security (L&MFSy) [see TAG 1.1 on Security Governance and Leadership].

6.4 Delivery of a capable security organisation involves many aspects of a dutyholder's business, including management arrangements that provide effective control and supervision of security operations, an understanding of security technology, effective quality control of processes and procedures, internal regulation and challenge, embodiment of a strong security culture across the organisation and the ability to understand and respond to legal requirements. The most effective and efficient organisations integrate security into their routine business delivery strategy and plans.

Regulatory Expectations

6.5 The regulatory expectation placed upon the dutyholder in order to demonstrate a capable organisation is that they will ensure that their security plan identifies:

- the governance structure and arrangements for security;
- a clear security organisational structure with corresponding roles and responsibilities including how organisational resilience will be achieved;
- the arrangements to control any change to the security organisational structure , or resources which may affect security;
- the arrangements to maintain a design authority capability to maintain knowledge of security facilities, equipment and arrangements;
- the arrangements to retain and manage the use of knowledge to ensure security requirements are understood and risks controlled through all activities; and,
- the arrangements to demonstrate the adequacy of financial resources.

FSyP 1 - Leadership and Management for Security	Capable organisation	SyDP 1.2
The organisation should have the capability to implement and maintain the security of its undertakings.		

Governance

6.6 Corporate governance is the system by which companies are directed and controlled. Boards of directors are responsible for the governance of their companies. It is essential that dutyholder boards treat security as an appropriate priority when providing strategic direction and leadership. More detailed guidance on regulatory expectations of dutyholders' governance can be found in the Governance and Leadership TAG [TAG 1.1].

Organisational Structure (Nuclear Baseline and Staffing Levels)

6.7 The Nuclear Baseline (NB) is the means by which the dutyholder demonstrates that its organisational structure, staffing and competencies are, and remain, suitable and sufficient to manage site security throughout the full range of the their business. It also provides the foundation from which organisational changes can be assessed in accordance with the dutyholder's arrangements specified in their security plan.

6.8 The dutyholder needs to show that it is able to maintain nuclear security arrangements approved through the security plan and remain legally compliant. This should not be a significant additional burden to the dutyholder, inasmuch as any organisation needs to know what resources, competencies and processes it needs to have in place to operate its business.

6.9 A second, important purpose is to provide a clear description of the currently intended staffing levels as a reference point or 'baseline' against which the dutyholder can assess the potential impact upon site security of proposed organisational changes. Therefore, the security plan should describe the components of dutyholder's security organisation.

6.10 In preparing its NB, the dutyholder should therefore consider all activities which have the potential to impact upon nuclear security, i.e. those activities with a positive impact and those which, if inadequately conceived or executed, could lead to an immediate or latent (direct but not immediate) detriment to nuclear security. This includes, for example, the governance of nuclear security, Intelligent Customer capability and drafting of security related documents, as well as frontline work. It should also include roles which have a direct contribution to nuclear security.

6.11 The dutyholder should be able to show that it understands the security roles that need to be delivered, and that these roles will be carried out by suitable and sufficient competent resource. It is not sufficient just to show that all roles are 'covered', but that those individuals in post can realistically carry these roles out to the required standard and capacity.

6.12 There are a number of methods and approaches for establishing staffing arrangements. ONR acknowledges that in some cases, staffing models may be based on approaches from predecessor or similar facilities, rather than a detailed, auditable analysis. In such cases, the inspector should request a comprehensive description of the staffing model and justification for its selection. In some instances, for example roles with a high potential impact on nuclear security, formal analysis may be required to demonstrate adequacy of proposed or existing staffing arrangements.

6.13 Details of the principles that should be assessed, and factors to be taken into consideration when determining whether the NB meets required standards and fulfils the claims and assertions made in the security plan, can be found in the Function and Content of the Nuclear Baseline TAG [NS-TAST-GD-065] [Ref. 13], and the Staffing

Levels and Task Organisation TAG [NS-TAST-GD-061] [Ref 12]. For reference the principles have been summarised in Appendix 1.

6.14 **Inspectors should consider**:

- In cases where staffing arrangements are based on an existing or predecessor facility, has the dutyholder considered and addressed any differences that may affect the appropriateness of the model (for example in design or operating concept or philosophy)?
- Where significant human-based claims are made in the security plan, has the dutyholder demonstrated that individual and team performance is supported by adequate supervision?
- In situations where staffing requirements vary depending on different operational modes or states and situations (e.g. night, weekends) can the dutyholder demonstrate that there are adequate resources for the most resource-intensive conditions feasible in each operational mode/state?
- If applicable, have the potential implications of sharing staff between multiple units or facilities been considered, including where staff are co-opted from a shared work pool? These include competence requirements (e.g. understanding of the security plan), workload (in normal and emergency conditions) and other factors such as the potential for errors related to operational or design differences between units/facilities).
- What reviews have been carried out to assess the adequacy of the staffing model, such as periodic security reviews, self-assessments, benchmarking or peer reviews? Have any deficiencies raised through the reviews been adequately addressed?
- Do the staffing arrangements allow sufficient time for training and development, and for rest and recovery, particularly during busy periods such as maintenance outages?
- Is there evidence of effective management of staffing levels above the required minimum, for example rapid call-out due to unexpected absence?
- Do qualitative and quantitative indicators support claims regarding adequacy of staffing levels and task organisation? Indicators of potential problems include:
    - high levels of maintenance or procedure modification backlogs;
    - events relating to staff shortages, work patterns, communication or co-ordination issues within or between teams, or inadequate supervision;
    - high levels of overtime;
    - deferrals or significant delays to nuclear security related work programmes;
    - large numbers of outstanding actions; and

- symptoms of personnel stress due to under or overload (e.g. high levels of sick leave, union grievances).

Change Control & Management of Change Principles

6.15 Where dutyholders have a security plan in place, amendments or changes to that plan should be approved prior to their implementation. The dutyholder's management of change arrangements should ensure that the nuclear security implications of a proposed change are fully considered and that risks arising from inadequate assessment and implementation of the change are recognised and suitably controlled. These arrangements should be part of a dutyholder's management system.

6.16 There are many drivers for organisational change and, without formal change management, a dutyholder may not immediately recognise the implications of a proposed course of action.

6.17 It is important that the full implications of a proposed change or a series of changes are rigorously assessed prior to implementation of the change(s). Senior managers often strive for short timescales when driving operational changes and in some cases deadlines can be unrealistic. This assessment is to guard against a failure to consider all relevant factors and potential dependencies between related changes, and the potential for 'salami slicing' in which a major change is decomposed into a series of lesser changes which are treated independently.

6.18 A Nuclear Industry Code of Practice (NICoP) on 'Nuclear Baseline and the Management of Organisational Change' recommends changes should be classified according to significance. Broad guidance for inspectors on the classification of organisational changes is given in Appendix 3. The level of assessment required should be proportionate to the potential nuclear security significance of the change. Additionally, inspectors should be familiar with T/AST/048 and T/AST/065 where extensive detail on the full change management process and the NB are contained including advice on what inspectors should consider when assessing the adequacy of dutyholders arrangements. Where dutyholders are able to demonstrate that their arrangements are consistent with the guidance in the NICoP, inspectors should regard this as meeting the expectations of this TAG. The NICoP is available on the website of the Security Director's Forum (www.safetydf.org.uk).

6.19 It should be noted that replacing one post holder with another post holder on a like-for-like basis need not constitute a trigger for the application of management of change arrangements. However, where a number of changes have taken place in the same area or there is a consequential effect on roles and responsibilities, the arrangements should be applied. Furthermore, multiple changes of SQEP personnel within the same work area should be avoided where possible.

6.20 There are some broad principles which underpin ONR's expectations of a dutyholder's management of change arrangements and these are laid out in Appendix 2.

Security Design Authority

6.21 The security arrangements at a nuclear site are the product of the activities of many organisations, and changes to those arrangements may occur periodically over the site's lifetime. Maintaining the level of security expected of a nuclear facility requires that changes to it must be made with full knowledge of the design and the security functions that need to be provided. This knowledge has to be retained in a form that is practically and easily available to the dutyholder over the full lifetime of the site.

6.22 A dutyholder should have a formal process to understand and maintain design knowledge and design integrity. That part of the dutyholder's organisation with the responsibility for, and the requisite knowledge to maintain, the design integrity and the overall basis for security of its nuclear facilities throughout the full lifecycle of those facilities is termed the 'Design Authority'[1].

6.23 Existing dutyholders should have a suitable and sufficient Design Authority capability and organisations seeking approval of a security plan to have credible programmes to develop this capability in a timely manner.

6.24 The Design Authority should have sufficient knowledge to understand the security arrangements for the site and to assess the impact of proposed design changes on the functionality, reliability and availability claims made in the security plan. The Design Authority should also have sufficient knowledge of any specific constraints that impact on the practical use of equipment and thereby need to be reflected in an effective design, such as restrictions in space, availability of site services, capability and limitations of security equipment sensors, the threat, etc. These factors should be considered at the same time as the generic design inputs, such as legislative requirements and security standards.

6.25 Ownership of the security plan and responsibility for understanding the function and performance of existing security arrangements should ordinarily reside with the operations function, rather than with the Design Authority. For new facilities within a nuclear site, the Design Authority may be the owner of the facility security plan during the design/construction phase prior to the operations function being established however this should comply with the extant wider security plan, otherwise prior to any modification being implemented, approval of a Temporary Security Plan should be sought from ONR. The Design Authority should be expected to maintain a security plan through-life, which should include:

- recording modifications to security arrangements effected to improve performance or made in the light of operating experience;
- approving design substantiations for any modification proposed;
- recording of operating experience which might impact the design across all security arrangements, and analysis thereof to identify trends and the need for essential equipment upgrades, tighter operating constraints etc;
- communication of the need for essential security equipment upgrades, tighter operating constraints etc; and,
- effecting essential research, through-life degradation testing etc. The purpose of this research is to support security arrangements to the end of the site's designed life or any potential life extension which may be requested by the operators.

6.26 ONR recognises that, for new plant, the vendor rather than the dutyholder may own the design. Where this is the case, ONR will expect the dutyholder to demonstrate how it proposes to acquire a suitable and sufficient Design Authority capability.

6.27 ONR also acknowledges that the dutyholder may not have all the detailed, specialised knowledge required of all the systems and components important to security within its Design Authority organisation. In such instances it may assign its responsibilities for some parts of the security equipment to other organisations such as those that

[1] Although the dutyholder may deliver the Design Authority function via a body with a different title, ONR expects that the Design Authority capability can be identified within the dutyholder organisation.

originally designed that equipment. Bodies with these responsibilities are termed 'Responsible Designers'. The dutyholder should be able to demonstrate how it intends to maintain a satisfactory contractual relationship to deliver the Responsible Designer service from the vendor for the foreseeable future, if this cannot cover whole plant life.

6.28 The dutyholder should retain sufficient knowledge of all aspects of the design to act as a Design Authority Intelligent Customer to enable it to understand the results of the Responsible Designers' work, and to understand the security implications of that work for the life of the plant. The dutyholder should also understand any implications from the design for other security systems on its site.

6.29 The roles of Design Authority and Design Authority Intelligent Customer should be part of the dutyholder's core capability and included in their Nuclear Baseline.

6.30 A summary of Security Design Authority Capability Principles can be found in Appendix 4. Details on what the inspector should consider when assessing a dutyholder's design authority including a detailed explanation of the Principles can be found in the Licensee Design Authority Capability TAG TAST-079 [Ref 14]

Knowledge Management

6.31 A key component of a capable organisation is one which has in place effective Knowledge management (KM) processes. KM is defined by the IAEA in TECDOC-1510 (Knowledge Management for Nuclear Industry Operating Organisations) [Ref 8] as:

> "An integrated, systematic approach to identifying, acquiring, transforming, developing, disseminating, using, sharing and preserving knowledge relevant to achieving specific objectives. Knowledge management helps an organisation to gain insight and understanding from its own experience. Specific activities in knowledge management help the organisation to better acquire, store and utilise knowledge"

6.32 As with all such concepts, the role of the leaders within an organisation cannot be overstated. The tone and level of expectations set by the most senior manager of an organisation will drive both the implementation and the results. KM is a vital component of change management and therefore a fundamental element of a capable organisation. As KM initiatives are undertaken, it is imperative that expectations and the reasoning behind those expectations are clearly communicated throughout the organisation. A spirit of knowledge sharing must pervade the organisation if the full potential of KM is to be realised. Sensitivity to the need for continual, consistent KM must become ingrained in the culture of an organisation. Therefore, a capable organisation will be able to demonstrate KM in its strategic planning; analysis and decision-making; implementation of plans; and, evaluation of results processes.

Inspectors should consider:

- Is there a strategy to ensure that as risks associated with losing persons with mission critical knowledge are identified, and arrangements for succession planning and developing leaders and managers are in place?

- Has a human performance improvement programme been established to continually identify opportunities to improve security performance and expand the knowledge of the organisation?

- Are strategies for knowledge transfer and retention developed and implemented to preserve unique knowledge and skills that could be lost through attrition or planned staffing changes?

- Does the culture of the organization promote the transfer of knowledge, particularly tacit knowledge among security personnel? Evidence of this culture is seen through the appointment of a knowledge champion and managers serving as role models for others to emulate regarding knowledge transfer.

- Does the dutyholder discourage knowledge transfer through rewarding employees based upon their being the sole source of critical knowledge and information, or does it reward employees for sharing their knowledge and information widely?

- Are managers personally involved in ensuring that the KM programme is developed, implemented, continuously improved and integrated with the organisation's overall management system? One example of this involvement is that managers feel accountable for the training, qualification, and performance of their personnel**.** A strategy should be developed to reward and recognize people for their contributions to growing the knowledge assets of the organisation.

- Does the dutyholder utilise benchmarking, which is an established policy to transfer knowledge, improve performance, and emulate best industry practices? Identification and correction of problems and use of operating experience, benchmarking, and self-assessment should be integral to the organisation's culture.

Adequacy of Financial Resources

6.33 The financial resources of a dutyholder are not ordinarily the focus of routine inspection activities nevertheless dutyholders should be able to demonstrate prudent fiscal planning and articulate how they will be able to achieve and maintain the security arrangements specified in the security plan. The security plan should set out the split in the security budget between operations, maintenance, asset management and investment which is to be reviewed during the dutyholder's annual review of security.

6.34 During routine regulatory engagement with dutyholder's, inspectors should be alert to indirect evidence that may indicate a reduction in the ability or willingness of the dutyholder to provide or maintain adequate financial resources to ensure security. Evidence may include failure to implement security improvements; security staff shortages that are not being filled; delays in delivering activities such as maintenance of security equipment etc. Should indications be found that investment in security-related plant or people may not be adequate to provide and maintain security, the Inspector should seek to establish whether it is attributable to other factors (for example difficulties in identifying SQEP resource; technical difficulties or disagreements etc.) and, if so, to progress the matter in the normal manner.

6.35 If the security issue cannot be resolved to the satisfaction of the Inspector, and financial resource issues are identified as a possible factor, this matter should be elevated to the relevant Superintending Inspector for consideration. It is anticipated that discussions will take place with the dutyholder to determine the cause of the issue and attempt to resolve it. This may entail a wider ONR review of the security plan;

annual financial accounts, plans for construction and key financial decision points; investment plans; lifetime plans, the nuclear baseline and other documents. If the issue cannot be resolved, and failure to comply with the security plan is determined, consideration may be given to engaging external expert financial advice to inform the process of establishing ONR's enforcement options. The need to take this course of action is expected to be rare.

6.36 Where the dutyholder's budget is controlled by another body (for example, the NDA or a parent organisation), financial (and other resourcing) arrangements are likely to be set out in contractual arrangements between the dutyholder and the controlling body. ONR may seek to examine these documents. ONR anticipates that the controlling body will co-operate with the dutyholder in ensuring the adequacy of the resources needed for security, and meet its obligations under NISR 2003 (as amended). The dutyholder, however, retains an absolute responsibility for site security.

6.37 Should a forensic accountancy service be needed, ONR has arrangements to access Government Forensic Accounting Services.

7. 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 TECHDOC 1510**. Knowledge Management for Nuclear Organisations. October 2006.

9. **IAEA Nuclear Energy Series NG-T-6.10**. Knowledge Management and its Implementation in Nuclear Organisations. April 2016

10. **IAEA SAFETY STANDARD S-G-3.1**. Application of the Management System for Facilities and Activities. July 2006

11. **ONR Document NS-TAST-GD-048 Revision 3** Organisational Capability

12. **ONR Document NS-TAST-GD-061 Revision 3** Staffing Levels and Task Organisation

13. **ONR Document NS-TAST-GD-065 Revision 2** Function and content of a Nuclear Baseline

14. **ONR Document NS-TAST-GD-079 Revision 2** Licensee Design Authority Capability

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

8. GLOSSARY AND ABBREVIATIONS

CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
L&MFSy	Leadership and Management for Security
NB	Nuclear Baseline
NDA	Nuclear Decommissioning Authority
NICoP	Nuclear Industry Code of Practice
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
NSyP	Nuclear Security Policy
ONR	Office for Nuclear Regulation
SQEP	Suitably Qualified and Experienced
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide

APPENDIX 1: PRINCIPLES OF A NUCLEAR BASELINE (NB)

A1.1. NB Principle 1:

The NB should consider the delivery and oversight of all activities which have the potential to impact upon security. This includes activities with a positive impact and those which, if inadequately conceived or executed, could lead to an immediate or latent detriment to security.

A1.2. NB Principle 2:

The NB should address the requirements of steady state conditions, periods of change and potential emergency situations at the current phase of the licensed facility's life cycle.

A1.3. NB Principle 3:

The Nuclear Baseline should demonstrate that the dutyholder's organisation has sufficient staffing and competencies to discharge its responsibilities for delivery and oversight of security as described in the security plan.

A1.4 NB Principle 4:

The dutyholder must demonstrate that it remains in control of nuclear security. The governance of security and Intelligent Customer capability are an intrinsic part of this demonstration.

A1.5 NB Principles 5 & 6:

Contract staff should appear as part of the NB resource when they are embedded within the dutyholder's organisation or meet the criteria for holding Intelligent Customer roles on behalf of the dutyholder.

A1.6 NB Principle 7:

Dutyholders should develop a set of Nuclear Baseline Indicators that provide evidence that the Nuclear Baseline has the right organisation, staffing levels and competences and that it is being managed effectively.

A1.7 NB Principle 8:

The dutyholder should have in place a process through which the NB is derived and managed.

A1.8 NB Principle 9:

The NB should be maintained as a living document and provide an accurate, current reference point against which security implications of proposed modifications to staffing levels/structures, workloads, and changed competence requirements can be assessed, in accordance with the dutyholders security plan.

APPENDIX 2: MANAGEMENT OF CHANGE PRINCIPLES

A2.1 MC Principle 1:

The arrangements should be robust, incorporated as part of the dutyholder's management system and applied to all activities that have the potential to impact on nuclear security.

A2.2 MC Principle 2:

The Board of the dutyholder should own and support the management of change arrangements and ensure that they are embedded throughout the organisation.

A2.3 MC Principle 3

The arrangements should reference the nuclear baseline and include a process for updating it on a regular basis.

A2.4 MC Principle 4

The arrangements should include an initial screening assessment to identify the potential security significance of a change proposal and establish a suitable categorisation for determining the level of analysis and justification.

A2.5 MC Principle 5:

The dutyholder should assess and justify the security implications of a proposed change commensurate with its potential impact, and monitor its implementation.

A2.6 MC Principle 6:

The dutyholder should periodically review the effectiveness of the overall arrangements and the changes that have been implemented.

APPENDIX 3: GENERAL GUIDANCE ON CLASSIFICATION OF ORGANISATIONAL CHANGE

A3.1 The approach to classifying changes may vary according to the dutyholder. The following example classifications are provided for illustrative purposes to guide the Inspector:

- Category 1 changes, which if inadequately conceived or executed, could result in a *major reduction* in the standards of security with the potential for on-site and off-site impact such as:
  - Wide ranging company or site changes that have the potential to affect the validity of, or basis on which, the nuclear site licence was granted.
  - Changes resulting in the granting of a new security plan.
  - Sale, acquisition or merger of a dutyholder organisation or a nuclear licensed site.
  - Changes involving more than one business unit, division or site.
  - Large-scale downsizing or outsourcing of a security significant function.
- Category 2 changes, which if inadequately conceived or executed, could result in a *significant reduction* in the standards of security with the potential to affect a large proportion of the whole of a site such as:
  - Changes that affect people within a whole facility.
  - Changes that affect a whole department or large groups of staff.
  - Changes that affect several layers of management.
  - Significant reduction in the size of a team that has key security role (i.e. the vetting team or security wardens).
  - Changes with significant potential to adversely impact on a site's emergency response.
  - Changes resulting in a significant transfer of key security accountabilities and responsibilities.
- Category 3 changes, which if inadequately conceived or executed, could result in a *minor reduction* in the standards of nuclear security with the potential to affect a single plant, department or business unit such as:
  - Changes that affect a small group of staff, such as part of a department.
  - Changes that mainly affect a single management layer.
  - Small reduction in the size of a team.
  - Changes in management accountabilities/responsibilities that have a small impact on security.
  - Transfer of responsibilities between departments/units.
- Category 4 changes with *negligible or no effect* on security such as:
  - Changes to organisational responsibilities that do not lead to a significant increase in the workload of any line manager or group of staff.

APPENDIX 4: DESIGN AUTHORITY CAPABILITY PRINCIPLES (DA)

A4.1 DA Principle 1:

The Design Authority should be a defined function within a dutyholder's organisation which is independent of operations and has a clearly defined reporting line to the Board of the licensee organisation.

A4.2 DA Principle 2:

The Design Authority should have the authority and the responsibility to approve or reject proposed design changes and concessions.

A4.3 DA Principle 3:

The Design Authority should have the capability to understand the totality of the design and security plan in the context of each stage of the full plant lifecycle.

A4.4 DA Principle 4:

The Design Authority should have the resources, capability and management processes to assess changes to the threat, and have the authority to recommend modifications to security structures, systems and components (SSCs) to ensure the security plan is maintained.

A4.5 DA Principle 5:

The Design Authority should have appropriate up to date knowledge, skills, experience and resources and have the authority to recommend modification to security SSCs to ensure the security plan is maintained.

A4.6 DA Principle 6:

The Design Authority should regularly assess and determine the continued adequacy of the site's security SSCs in meeting the requirements of the security plan and have the authority and responsibility to respond to the issues identified.

A4.7 DA Principle 8:

Where the Design Authority does not have the detailed, specialised knowledge required of all the SSCs important to security it may choose to assign those responsibilities to 'Responsible Designers' using the supply chain.