ONR GUIDE			
COOPERATION OF DEPARTMENTS WITH RESPONSIBILITY FOR DELIVERING VETTING AND ONGOING PERSONNEL SECURITY ARRANGEMENTS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-8.1 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19079. (2017/108460)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 2). 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 the exercise of their regulatory judgement during assessment activities relating to how the dutyholder's departments with responsibility for delivering the BPSS, NSV and Ongoing Personnel Security, for its employees and contractors, cooperate and work effectively in conjunction with one another. 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 workforce trustworthiness to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

3.3 Regulations 9, 17(3) and 22(7) (d) of NISR relate to workforce trustworthiness and have been included at Appendix 1 to this TAG. Furthermore, due consideration in relation to the treatment, use and the holding of personal information must also take into account the following legislation:

- Data Protection Act 1998
- Human Rights Act 1998
- Rehabilitation of Offenders Act 1974
- Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975
- Rehabilitation of Offenders (Exclusions and Exceptions) (Scotland) Order 2003
- Rehabilitation of Offenders (Northern Ireland) Order 1978
- Equality Act 2010
- Protection of Freedoms Act 2012

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 3) and the IAEA Nuclear Security Fundamentals (Reference 4). 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 should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation. Essential Element 12 of the Nuclear Security Fundamentals refers to developing, fostering and maintaining a robust nuclear security culture and to establishing and applying measures to minimise the possibility of insiders becoming nuclear security threats.

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 14). Further detail at the operational level is contained in an Implementing Guide on Preventive and Protective Measures Against Insider Threats (NSS 8) (Reference 6), in particular Sections 3 and 5. An Implementing Guide on Nuclear Security Culture (NSS7) (Reference 5) contains further information on establishing workforce trustworthiness (Section 4.3(i)).

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 Security Delivery Principle 8.1 – Cooperation of Departments with responsibility for delivering vetting and ongoing personnel security arrangements, in support of Fundamental Security Principle 8 – Workforce Trustworthiness. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 7) is supplemented by the "Cabinet Office SPF Personnel Security supplement (Reference 15), HMG Baseline Personnel Security Standard Guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors"

(Reference 9). It describes the Cabinet Office 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 dutyholders are presented with a coherent set of expectations for the protection of nuclear material and nuclear facilities and SNI, and for 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 that require a classification and the level of classification to be applied.

6. ADVICE TO INSPECTORS

National Policy and Guidance Related to Cooperation of Departments

6.1 **Cabinet Office**. The Baseline Personnel Security Standard (BPSS) and National Security Vetting (NSV) policy is determined by Cabinet Office as the National Security Authority for the United Kingdom.

6.2 **HMG Policy Expectations**. The Statement of HMG Personnel Security and NSV Policy (as contained within Reference 10) advises that there will be checks of “relevant personnel records held by the employing department or company” and “ the process may also take account of financial circumstances generally…[and]…any medical considerations that could give rise to security concerns”. This, in conjunction with the paragraphs that follow, sets an expectation for relevant departments, including HR and medical, to work effectively together.

6.3 Reference 10 further advises that “security clearances may be refused or withdrawn where…personal circumstances, current or past conduct indicate that an individual be susceptible to pressure or improper influence…instances of dishonesty or lack of integrity cast doubt upon an individual’s reliability…or other behaviours or circumstances indicate unreliability”. It also states,” the national security vetting process provides an assessment of the vetting subject at the time the process is carried out, but active ongoing personnel security management is required to ensure that a security clearance maintains its currency. As a minimum this will involve active consideration of the vetting subject’s continuing conduct in respect of security matters”. A dutyholder’s consideration of a subject’s continuing conduct is most effective when the relevant departments work cooperatively.

6.4 **HMG BPSS Guidance**. BPSS guidance (Reference 9) states “It is strongly encouraged that HR and Security units work closely to ensure the effective and consistent application of the guidance.” It further adds “the necessary checks at the recruitment stage only offer a snapshot. It is essential that HR divisions and line managers continue to apply good personnel security management after recruitment to identify any changing or suspicious behavioural patterns in staff that might suggest unreliability or conflict of interest.” This guidance restates the policy view that the effectiveness of personnel security and employment controls are greatest when relevant departments work together. In this respect the term staff is to include both the employee and contracting communities. TAG 8.2 gives a detailed explanation of the definition of staff (or employees) and contractors.

6.5 **NSV Questionnaires**. Information requested in the NSV questionnaires (References 12 and 13) relating to:

- medical conditions (most notably serious medical and psychological);
- the misuse of alcohol or drugs;
- financial difficulties;
- conduct liable to lead to susceptibility to pressure or improper influence;
- criminality; and
- the sponsor conducting a record check against employee/contractor records;

indicates the broad range of information that dutyholders should consider in respect of ongoing personnel security. Thus it implies the need for the work of relevant departments to be properly integrated.

Regulatory Expectation

6.6 The regulatory expectation is that dutyholders will ensure their security plan identifies arrangements that clearly integrate the work of all departments with a responsibility for pre-employment screening, NSV or ongoing personnel security in order to maintain a trustworthy workforce and minimising the possibility of insiders becoming nuclear security threats.

FSyP 8 - Workforce Trustworthiness	Cooperation of Departments with Responsibility for Vetting and Ongoing Personnel Security	SyDP 8.1
Dutyholders should ensure that their human resources, occupational health and security departments are integrated to facilitate effective vetting and ongoing personnel security arrangements for the workforce (staff and contractor community).		

7. ARRANGEMENTS FOR COOPERATION BETWEEN DEPARTMENTS

7.1 Inspectors should consider that personnel security controls are effective only when there is close cooperation between the human resources (which includes Occupational Health) and security departments. In light of this, there are two aspects which are considered to be fundamental if dutyholders are to demonstrate adequate cooperation between such departments and these are detailed below.

- A formal mechanism to report to the security department incidents or concerns that identify a potential trustworthiness issue, or events which may impact the pass control system, or cause doubt as to the belief on the ongoing suitability of an individual to hold a clearance. Different reporting thresholds will exist depending on the level of clearance held.
- Human Resources (HR) (and potentially Occupational Health (OH)) attend relevant training (such as the CPNI courses – Personnel Security Risk Assessment and Resolving Suspicions about Employees of Concern) and are familiar with personnel security products available through the CPNI website (Reference 11).

7.2 In addition to the fundamental considerations given above, the following paragraphs provide guidance on specific measures that also contribute towards the effective cooperation between departments in support of personnel security arrangements:

- Management structures and procedures, with corporate oversight, that provide for effective information sharing and cooperation between HR (including OH & Training departments) and security teams. Management arrangements should provide policies and procedures for detecting, reporting, responding to and handling incidents relevant to ongoing personnel security, including disciplinary measures that are well-communicated to, and understood by, staff.

- Management structures and procedures, with corporate oversight, that provides for effective personnel security relationships between the dutyholder security department and contractor organisations.

- A formal mechanism to report to the security department, to ONR or both, incidents or events of potential personnel security concern which may warrant greater oversight of an individual. Different reporting thresholds will exist depending on the level of clearance held.

- Establishment of a forum for the Security, HR and OH departments to discuss concerns and review the security culture and ongoing personnel security awareness.

- Inclusion of the security department as a stakeholder in formulating training and/or learning and development products that contain personnel security messages.

- Inclusion of the security department as a stakeholder in formulating security guidance associated with managerial and supervisory responsibilities including whether such guidance is provided.

- Inclusion of the security department as a stakeholder in formulating HR policies where there is, or should be, personnel security considerations. For example job advertisements and offer letters that should include clearance requirements.

- Adoption of HR policies that appropriately consider consent in relation to the sharing of information. For example drug and alcohol testing where the reporting of positive tests for NSV holders is mandated by ONR as the Vetting Authority.

- The engagement of the procurement department to ensure personnel security expectations, including ongoing assessment, are included in contractual arrangements at both the tender and formal contract award stages.

- Arrangements are in place for sharing, between relevant departments and line managers, details of caveats or recommended conditions of employment placed against the individual's clearance, and requiring ongoing management.

Inspectors should consider:

- Is there appropriate corporate governance and oversight of cooperation between the relevant departments with responsibility for personnel security

within both the dutyholder organisation and, as appropriate, the supply chain?

- Does the dutyholder have relevant internal assurance policies and processes to evidence the bullet above?
- What evidence is there of cooperation and how have relevant departments influenced one another?
- What protocols exist between relevant departments?
- Are personnel in roles that have responsibility for personnel security suitably qualified and experienced, and are the requirements for relevant professional training courses formally identified and demonstrably complete?
- Are relevant departments, including the supply chain, aware of sources of guidance supporting an effective ongoing personnel security culture?
- Do recruitment, training/learning and development, conditions of service, and exit policies/guidance/procedures support a coordinated approach to personnel security by a dutyholder?
- Do tender and contract award terms give sufficient weight to integrated personnel security procedures, policies and expectations?
- Are line managers properly informed and trained on ongoing personnel security arrangements?

8. LIMITATIONS

8.1 The Data Protection Act 1998 and common law, under the law of confidence, contain obligations, with regard to patient confidentiality, which apply to doctors and others dealing with medical issues. In order to demonstrate that it is lawful to disclose medical information, the doctor or medical staff will need to carry out a balancing act between the importance of the purpose for which the information is being disclosed and the privacy of the individual and sensitive nature of the information being disclosed. In some cases this could justifiably limit the extent to which the work of different departments may be integrated and inspectors are to be mindful of this.

9. REFERENCES

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

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

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

4. **Nuclear Security Series 20 - IAEA Nuclear Security Fundamentals** http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

5. **IAEA Nuclear Security series No 7 – Nuclear Security Culture** http://www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf

6. **IAEA Nuclear Security Series No 8 – Preventative and Protective Measures against Insider Threats** http://www-pub.iaea.org/MTCD/publications/PDF/pub1359_web.pdf

7. **HMG Security Policy Framework**.

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

9. **HMG Baseline Personnel Security Standard – Guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors** www.gov.uk/government/uploads/system/uploads/attachment_data/file/365602/HMG_Baseline_Personnel_Security_Standard.pdf

10. **HMG Personnel Security Controls** - www.gov.uk/government/uploads/system/uploads/attachment_data/file/299547/HMG_Personnel_Security_Controls.pdf

11. **Centre for the Protection of National Infrastructure - Personnel Security references** www.cpni.gov.uk/advice/Personnel-security1/

12. **Counter Terrorist Check / Security Check Questionnaire**

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/585924/20160927-Form_NSV001_v0.2-U.pdf13. **Developed Vetting Questionnaire** https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/585926/20160927-Form_NSV002_v0.2-U.pdf

14. **INFCIRC/225 IAEA – The Physical Protection of Nuclear Material** https://www.iaea.org/publications/documents/infcircs/physical-protection-nuclear-material

15. **Cabinet Office SPF Personnel Security supplement, version 6.4, dated November 2015**. (OFFICIAL – SENSITIVE).

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

10. GLOSSARY AND ABBREVIATIONS

BPSS	Baseline Personnel Security Standard
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
HR	Human Resources
IAEA	International Atomic Energy Agency
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
NSV	National Security Vetting
NSyP	Nuclear Security Policy
OH	Occupational Health
ONR	Office for Nuclear Regulation
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide

APPENDIX 1 – EXTRACT OF NISR 2003 CONCERNING WORKFORCE TRUSTWORTHINESS

Regulation 9: "The responsible person in relation to each nuclear premises must ensure that each of his relevant personnel in relation to the premises who -

a) Is specified in the approval security plan for the premises as requiring investigation and assessment as mentioned in regulation 4(3)a, or

b) Falls within a description of persons who are so specified,

is a person who has been assessed, in accordance with a process that has been approved by the ONR, to be of suitable character and integrity, having regard to the need to ensure the security of the premises and the material, equipment and information mentioned in regulation 4(2).

Regulation 17(3): "An approved carrier must ensure that each of his relevant personnel who-

a) Is specified in his approved transport security statement as requiring investigation and assessment as mentioned in regulation 16(3)(a), or

b) Falls within a description of persons who are so specified,

is a person who has been assessed, in accordance with a process that has been approved by the ONR, to be of suitable character and integrity, having regard to the need to ensure the security of the material, information and premises mentioned in Regulation 16(3)(a).

Regulation 22(7)(d): "A person to whom this regulation applies must – ensure that each of his relevant personnel who-

(i) Is specified in a direction given under paragraph (7)(b) as a person whose suitability requires investigation and assessment by the Secretary of State; or

(ii) Falls within a description of persons who are so specified,

is a person who has been assessed, in accordance with a process that has been approved by the ONR, to be of suitable character and integrity, having regard to the need to ensure the security of any sensitive nuclear information, uranium enrichment equipment or software within the possession or control of the person to whom this regulation applies.