ONR GUIDE			
WORKFORCE TRUSTWORTHINESS			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-8.0 Revision 0		
Date Issued:	January 2018	**Review Date:**	January 2021
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	TRIM Folder 4.4.2.20789. (2017/456637)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 01/18

1 INTRODUCTION

1.1 The Nuclear Industries Security Regulations (NISR) 2003 (Reference 7.1) contains requirements for responsible persons to make certain arrangements including standards and procedures to ensure the security of the nuclear premises, Nuclear Material (NM) or Other Radioactive Material (ORM) stored on the premises, Sensitive Nuclear Information (SNI) and standards and procedures for the transportation of Category I - III NM.

1.2 Regulation 4 of NISR requires there to be an approved security plan for each nuclear premises[1] which details those arrangements for the protection of NM/ORM and SNI, including contingency plans. Regulation 7 places the requirement for the dutyholder to maintain arrangements in accordance with the approved plan. Similarly, transporters of Category I-III quantities of NM are required to detail their security arrangements in an approved Transport Security Statement in accordance with Regulation 16 and Regulation 17 requires them to maintain those arrangements. For the purposes of this guide, the term security plan will be used to refer to both approved documents.

1.3 The Office for Nuclear Regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 7.2) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

1.4 To assist inspectors, ONR produces a suite of guides to assist them in making regulatory judgements and decisions in relation to the adequacy of compliance. This inspection guide is one of the suite of documents provided by ONR for this purpose.

2 PURPOSE AND SCOPE

2.1 Security plans should be structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guide is to facilitate a consistent and effective approach to inspecting compliance with the arrangements described in the plan and detailed in the underpinning documentation concerning FSyP8 – Workforce Trustworthiness.

2.2 The judgements made by the inspector will primarily relate to the efficacy of the implementation of arrangements described in evidence that supports the security plan to ensure that associated arguments are fully substantiated. However, ONR takes a sampling approach to regulation and it is possible that elements of evidence within the plan or underpinning the plan were not subject to assessment as part of the approval process. Therefore, when reviewing or inspecting evidence as part of the intervention, the judgement may relate to the adequacy of the arrangements which support the approved plan. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 The guidance should not be regarded as either comprehensive or mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections. This guidance consists of elements which will help inspectors

[1] As defined by Regulation 2 of NISR 2003.

plan their inspection programmes and workforce trustworthiness compliance inspections.

2.4 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) and the International Atomic Energy Agency (IAEA) Nuclear Security Fundamentals. Further guidance is available within IAEA implementing guides and technical guidance.

2.5 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. SyAPs transposes this requirement in the UK and this guidance considers the relevant aspects of workforce trustworthiness.

3 RELATION 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 This guidance is to inform inspectors what they should inspect to determine the adequacy of dutyholder’s arrangements relating to workforce trustworthiness. Furthermore, dutyholder’s arrangements should take into consideration the following legislation in relation to the treatment, use and holding of personal information as it relates to pre-employment checks and ongoing personnel security management:

- Data Protection Act 1998
- General Data Protection Regulations (in force May 2018)
- 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 OVERVIEW OF FUNDAMENTAL SECURITY PRINCIPLE 8 : WORKFORCE TRUSTWORTHINESS

4.1 FSyP 8 is concerned with the implementation and maintenance of a trustworthy workforce within the dutyholder organisation. It states that “dutyholders must implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity”.

4.2 SyDP 8.1 considers the co-operation of departments with responsibility for delivering screening, vetting and ongoing personnel security: and says that “Dutyholders should ensure that their Human Resources (HR), occupational health (OH) and security departments cooperate to facilitate the effective screening, vetting and ongoing personnel security arrangements for the workforce (staff and contractor community)”. It notes that each of these departments should ensure they have, Suitably Qualified and Experienced (SQEP) personnel, an understanding of the issues and concerns that could indicate an individual may pose a security risk, protocols for the sharing of information, and a forum to discuss changes to personnel security policies and promoting a personnel security culture. Such arrangements must include HR and OH departments in the supply chain.

4.3 SyDP 8.2 concerns pre-employment screening and national security vetting and says “dutyholders should deliver the appropriate combination of recruitment checks and vetting to satisfy themselves of the honesty and integrity of their potential workforce” (staff and contractor community), as well as the right to work. The HMG Personnel Security Policy document requires all those seeking to achieve National Security Vetting (NSV) to first hold a Baseline Personnel Security Standard (BPSS). Inspectors will need to be mindful that dutyholders may outsource some of the BPSS checks to screening providers, or where the dutyholder is the contracting authority, the employer may carry out many of the checks. Where individuals are sponsored for NSV, dutyholders should establish robust arrangements that manage its sponsorship in compliance with current Cabinet Office guidance and additional ONR expectations as articulated in SyAPs Annex M and concerning the acquisition of overseas police certificates.

4.4 SyDP 8.3 considers ongoing personnel security, often referred to as “aftercare”. It says “dutyholders should implement and maintain on-going personnel security management arrangements and procedures to remain assured about their workforce and to mitigate the risks from insiders”. Dutyholders should establish robust arrangements that manage the delivery of NSV sponsorship in compliance with current Cabinet Office guidance and additional ONR requirements. Medical concerns may at times be a potential security (and/or safety) concern, and OH departments will need to consider the common law principle of medical confidentiality to determine if a disclosure threshold is achieved. HR will wish to consider the consequence of disciplinary or grievance actions which may result in disaffection, again re-emphasising the importance of co-operation of relevant departments (including within the supply chain).

4.5 To help individuals manage potential vulnerabilities the dutyholder and its supply chain organisations should have in place appropriate policies e.g. Employee Assistance Programmes, Benevolent Funds, and Reporting/Whistle-Blowing Hotlines. These policies should encourage an inclusive and supportive culture, underpinned by policies on the consequence of unacceptable behaviour e.g. Harassment & Bullying, Equal Opportunities and Diversity, Drug and Alcohol Misuse.

4.6 Board or similar senior level endorsement of co-operation between relevant departments for ongoing personnel security oversight should exist and encompass the appropriate engagement with the supply chain. This endorsement should also ensure that personnel security has an appropriate profile in workforce engagement surveys, the site induction programme and learning and development activities.

5 GUIDANCE ON THE INSPECTION OF WORKFORCE TRUSTWORTHINESS ARRANGEMENTS

5.1 ONR expects its inspectors to be able to deliver inspection of nuclear site licensees or other dutyholders in a consistent manner and expects similar outcomes for similar findings. The same basic elements should be applicable to an inspector in any of the delivery programmes including conducting a programme of personnel security interventions to influence personnel security behavioural changes across the industry. ONR-INSP-GD-064 Revision 2 (Reference 7.16) provides guidance for all inspection activities undertaken by ONR inspectors.

5.2 For all of the major sites and facilities, an annual personnel security integrated intervention strategy (IIS) plan exists which describes how the strategy is realised through a series of planned inspections.

5.3 For more detail on IIS plans, see ONR GUIDE GD-059 (Reference 7.17). Inspections involve the examination of documentation and arrangements of the facility, its security processes, operations and organisation underpinning the security outcomes in its security plan. A sampling approach should be used when planning inspections which will be based on the confidence the inspector has of the organisation's approach to personnel security and workforce trustworthiness, the risks and vulnerabilities of activities covered by the security plans and recent events or operating experience at the facility.

5.4 **Planning** - the inspector should be clear as to the purpose of the proposed intervention and why is it being considered; which could include regulatory intelligence, divisional strategy, routine compliance, permissioning or another reason that is driving the intervention. Once these initial considerations are understood, the inspector should be in a position to define and agree the outcomes and outputs of the intervention. Where delivery of these objectives identifies the requirement for additional regulatory resources, support from other specialists should be sought.

5.5 **Preparation –** Prior to the inspection, the inspector should ensure that they obtain and review the organisation's current policies regarding the ongoing personnel security culture. Such policies will typically include those on harassment and bullying; equality and diversity; employee assistance programme and benevolent funds; social networking; reporting hotlines; and drug and alcohol testing.

5.6 It is important that the inspection is organised with the dutyholder at the correct level, ensuring that where joint inspections (which may include an external organisation such as the Centre for the Protection of National Infrastructure (CPNI)) take place, the dutyholder is provided with details of all participants. A site coordinator or contact should also be nominated and depending on the site or organisation concerned, this could be a personnel security manager, human resources manager, or regulatory liaison.

5.7 An agenda for the inspection should be developed by the inspector and agreed with the site coordinator or contact. Early issue of the proposed agenda allows the dutyholder to ensure the correct people are available. The inspection plan and the associated contacts should be agreed before the delivery phase. This plan should allow for visits to the organisations or supply chain premises off the licensed site, where personnel hold a BPSS or NSV clearance.

5.8 **Delivery** – Inspections can be completed by individual inspectors or by teams of ONR inspectors. In some instances, personnel security Inspectors may be assisted by ONR divisional delivery support personnel. Paired or teamed inspections can be completed

with other regulators and may also occasionally include staff from other organisations (such as the Centre for the Protection of National Infrastructure), who provide a contribution in an advisory capacity. In all cases, it should be clear during the planning stage who is leading the inspection and who is preparing the inspection record.

5.9 Inspectors should take into account that the risk based approach applies to the assessment of an individual's suitability to achieve a certain level of NSV. This may include management of risk through the application of caveats.

5.10 The BPSS grants routine access to OFFICIAL and occasional access to SECRET, the Security Check (SC) routine access to SECRET and occasional access to TOP SECRET, and Developed Vetting (DV) routine access to TOP SECRET information and assets. The levels of clearance, including Counter Terrorist Check (CTC), have differing ongoing personnel security reporting requirements and inspections should focus primarily on where the greatest risks exist by way of the individual's access to information and assets. Inspectors should determine whether the organisation's minimum clearance levels comply with those mandated in SyAPs.

5.11 Whilst organisational ongoing personnel security measures should be assessed at each inspection, inspectors should ensure that mandated ongoing personnel security reporting requirements e.g. Annual Security Appraisal Forms (ASAFs) for DV holders, Change of Personal Circumstances Questionnaires (CPC) for NSV holders, noting the additional requirement in relation to co-residents at DV, are assessed. In that regard one to one challenges with the workforce would focus on a greater proportion of NSV holders as opposed to BPSS holders.

5.12 Equally, noting the time constraints that may exist, any assessment concerning the visibility of the ongoing personnel security culture should focus first on areas where assets have a higher degree of sensitivity or where personnel who have access to these assets work or congregate e.g. canteen or contractor cabins. They should also take account of emergent themes arising from staff surveys or feedback.

6 GUIDANCE ON INSPECTION OF THE IMPLEMENTATION OF WORKFORCE TRUSTWORTHINESS ARRANGEMENTS

6.1 The arrangements developed by an organisation to create and sustain a robust personnel security culture should contain a number of discrete elements, including: the co-operation of departments with responsibility for delivering screening, vetting and ongoing personnel security; adherence to the pre-employment screening and national security vetting process; and implementing and maintaining on-going personnel security management, arrangements and procedures. Guidance on the inspection of the arrangements made by the dutyholders for these elements and their implementation is defined in the following sections.

SyDP 8.1 - The co-operation of departments with responsibility for delivering screening, vetting and ongoing personnel security

6.2 The organisation should ensure that their human resources, occupational health and security departments take a collaborative approach to personnel security. This approach should ensure that for staff, recruitment processes ease the facilitation of the BPSS, and for NSV, relevant issues of security interest are drawn to the attention of the security department.

6.3 For the supply chain, the dutyholder's security manager should have established relevant points of contact within the supply chain organisation who are suitably qualified and experienced to validate identity documentation for the purposes of

employment; and who are able to advise on human resources and health concerns of security interest.

6.4 Inspectors should consider –

- How frequently the organisation's HR, OH and security departments meet to discuss personnel security concerns or personnel security policy developments and whether that periodicity is adequate? Are formal records of such meetings made and retained?
- Is there is a collaborative approach to developing and amending relevant policies within the organisation e.g. drug and alcohol testing, Reporting Hotlines? How is this demonstrated?
- Have HR staff received appropriate personnel security training (e.g. CPNI) to raise awareness of personnel security considerations. This may include pre-employment screening; personnel security risk assessment; and, resolving suspicious behaviours? How is training attendance recorded?
- Are training requirements stipulated in the nuclear baseline / organisational policy and specified in relevant job descriptions?
- Are the HR and OH departments (recognising the common law duty of medical confidentiality) aware of issues that may indicate a personnel security concern and how well are they understood by their representatives?
- Is there is an evidence base of relevant information being shared?
- Does the organisation's security department have effective liaison arrangements in place with supply chain organisations? And do they require the latter to report issues that may be of personnel security concern?
- What personnel security awareness activities does the organisation deliver to its supply chain organisation? How and to whom is this delivered?
- Does the organisation receive Management Information about usage of employee assistance programmes and / or reporting hotlines? Is this information used to inform targeted security messaging?

SyDP 8.2 - Pre-employment Screening and National Security Vetting

6.5 The processes that underpin the BPSS and NSV clearances are mandated in HMG published guidance. For the BPSS, this is the Cabinet Office publication 'HMG Baseline Personnel Security Standard' and for NSV, the OFFICIAL – SENSITIVE 'Personnel Security Supplement to the Security Policy Framework'.

6.6 In addition to the HMG published guidance, ONR requires that overseas police certificates are provided at BPSS where there is 6-month absence, or more, within 3 years of the BPSS application and at NSV where there is a 12-month absence, or more, within 5 years for DV/SC or 3 years at CTC and where more than 6 months is spent in one country.

6.7 Personnel validating documentation as part of the BPSS should be suitably qualified and experienced with records maintained that evidence any learning and development activities attended or undertaken.

6.8 Where dutyholders use the service of a third party to undertake background screening to provide evidence which supports the BPSS process, the dutyholder should ensure that the standard achieved meets, and continues to meet relevant HMG standards.

6.9 Where dutyholders are authorised to approve the BPSS, they should be alert to indicators that suggest conditions to the terms of the employment may be required e.g. participation in a drug or alcohol testing programme.

6.10 Individuals sponsoring NSV applications should ensure that with each application an assurance is obtained from the current employer that there are no items of security interest to be considered by the vetting service provider or the vetting authority as the decision maker.

6.11 Visitors to sites do not necessarily require BPSS screening or a national security vetting clearance, though appropriate identity checks and reporting of such visits to ONR may be required dependent on the nature of the visit.

6.12 Inspectors should consider –

- Is the BPSS process compliant with at least minimum standards as published in Cabinet Office guidance?
- Are personnel who are verifying ID documentation suitably qualified and experienced to assess this evidence?
- Are overseas police certificates obtained and are they checked during the sampling of casework?
- Does the dutyholder use an external screening provider? Has the veracity of the service been established and what ongoing oversight of the service exists?
- Does the BPSS decision maker refer casework identified through sampling and outside their authority to ONR for approval? Do they apply appropriate conditions of employment where concerns arise within their signing authority?
- Do arrangements exist to determine the level of NSV clearance (where required) needed?
- Where an individual is sponsored for an NSV clearance, does the dutyholder obtain assurances from current employers that there are no items of security interest? How is the outcome of this request recorded?
- Are the reporting processes for visitors detailed in the OFFICIAL SENSITIVE annex to SyAPs being followed?
- Do access control systems reflect the level of clearance held and the appropriate expiry date? Is this implemented on the access control system?

SyDP 8.3 - Ongoing Personnel Security

6.13 Whilst there are no formalised ongoing personnel security arrangements for BPSS holders, holders of NSV clearances are required to notify certain changes in personal circumstances. This involves the completion of a questionnaire for changes relating to a change in living arrangements, nationality, criminality and financial circumstances.

6.14 All DV clearance holders are required to complete an ASAF which is in two parts Part 1 completed by the subject and Part 2 completed by their line manager. This ASAF should be returned through the organisation's security department unless the subject and/or line manager withhold their consent for the security department to see the content, in which case it must be sent directly to ONR as the vetting authority. Where security departments view the content of the completed ASAF and concerns are raised, they should put in place appropriate mitigation measures.

6.15 Where organisations have drug and alcohol testing procedures in operation, notifications of positive results for NSV holders only should be made to ONR.

6.16 The NSV security questionnaire asks questions at CTC/SC level on whether subjects have had or have serious medical or psychological illnesses or whether they are or have been a habitual user of addictive substances (e.g. drugs or alcohol). At DV, applicants are asked: whether they are currently taking medication; whether the subject has suffered at any time from clinical depression, mental illness, nervous breakdown/nervous debility, serious medical or psychological issues; conditions that may cause momentary loss of consciousness; a habitual user of addictive substances; or other health issues which may affect suitability to access sensitive information or assets. In that regard, dutyholder OH departments should consider being mindful of the common law duty of medical confidentiality and its disclosure arrangements where there is a potential security concern. Inspectors should be satisfied that arrangements exist for OH to discuss such cases with the security department.

6.17 Dutyholder HR departments should be mindful that work related grievances may cause parties to feel demoralised and potentially disaffected, as can disciplinary cases which may also be indicative of poor security behaviours. Conditions of employment may require the internal reporting by individuals of convictions or bankruptcy, for which NSVS reporting requirements are also mandated. Arrangements should exist to discuss such cases with the security department and inspectors should review the evidence base.

6.18 Employee Assistance Programmes, Reporting Hotlines and Benevolent Funds are potential avenues for the workforce to address concerns e.g. legal issues; financial problems; marital concerns; or poor practices which may, particularly if they escalate, become a potential security concern. Organisations should have given due consideration to the introduction of employee support programmes, with associated policies e.g. harassment and bullying, equal opportunities, diversity and adequately promote these across the organisation. Where non-attributable information is collated, the inspector will wish to see that this information has been shared between HR, OH and the security department to identify trends and to inform any ongoing personnel security strategy.

6.19 Security departments should have effective relationships with their supply chain organisations to ensure any security concerns or risks are identified, communicated and mitigations put in place. Points of contact would be expected to include those in supply chain organisations who have responsibility for HR (including occupational health) and security.

6.20 An organisation's employee assistance (and associated) programme may only apply to its staff. Security departments should be clear as to what policies exist within its supply chain organisations and how such policies are promoted and usage reports acted upon.

6.21 Organisations should ensure that where NSV are due for renewal, that the renewal request is submitted in advance of the current clearance expiring.

6.22 Where a caveat (or at BPSS, condition of employment) is applied to a clearance, the organisation should appropriately manage it. The security department should implement adequate procedures and processes to ensure that a caveat is enforced, communicated and managed correctly through the period for which it remains applicable.

6.23 The security department should work collaboratively with appropriate departments (e.g. HR) to determine the personnel security content of induction programmes and the annual learning and development strategy including intended surveys of the workforce.

6.24 Arrangements should exist for NSV holders to report forthcoming overseas travel, both on business or pleasure, and for an appropriate briefing (and potentially debriefing) to be delivered on secure behaviour commensurate with the risk profile of the country.

6.25 On termination of employment, dutyholders should have arrangements in place that ensure that an individual's access rights to the site and any information systems (including remote) are removed.

6.26 Inspectors should consider:

- Does the dutyholder remind NSV holders when they are required to complete CPC questionnaires and how does this reminder take place?
- Does the dutyholder have adequate mechanisms in place to ensure that CPCs are completed by personnel where required? One potential option may be to reconcile the expected financial charge with the monthly casework invoice. Is the completion formally acknowledged against locally held vetting records?
- Does the dutyholder ensure that all DV holders complete an ASAF and where these are not returned upon first request, that they are pursued with non-compliance cases reported to ONR?
- Does the dutyholder triage the ASAF so immediate mitigations can be put into place rather than waiting on the completion of the ONR assessment? What mitigations can the organisation evidence?
- Does the drug and alcohol testing policy make it clear that positive results for NSV holders will be reported to the vetting authority?
- Does the dutyholder report positive drug and alcohol tests for NSV holders to ONR? Does the OH department notify the security department of positive results?
- Does the occupational health department take security factors into consideration when considering workforce ailments and if so, does it balance the common law duty of medical confidentiality against disclosure? What thresholds does the OH representative advise are considered?
- Is the HR department aware of the potential security consequences of HR interventions including exit interviews and where concerns arise, are they discussed with the security department? What is the evidence base of reporting such concerns?
- Are supportive employment policies and assistance programmes adequately promoted in the workplace? Have these been seen on the organisation's intranet, notice-boards, back of toilet cubicle doors etc?

- Is data on the number and volume of calls to Employee Assistance programmes and Benevolent Funds shared with HR, OH and security, particularly to support ongoing personnel security themes? How has such information informed ongoing personnel security strategy?

- How are potential security concerns in the supply chain identified and discussed between the supply chain HR and OH departments and the dutyholders security departments?

- How do supply chain organisations deliver employee support services to their workforce and how is information on utilisation used to inform ongoing personnel security campaigns? What is the visibility of such measures following a walk-through of supply chain premises?

- How aware is the dutyholder of its supply chain organisation's ongoing personnel security measures? How is awareness recorded?

- Does the dutyholder have a process that ensures requests for a renewal of a clearance are generated before the current clearance expires? What reports are run to support the prompt to renew?

- Where a clearance has been issued with a caveat or condition of employment, how is that caveat managed, are relevant parties notified, and are required actions (e.g. requiring a basic disclosure) followed?

- Does the security department work collaboratively with appropriate departments (e.g. HR, Training) to develop the content of induction programmes, the annual learning and development strategy, and the content of staff surveys? What has been the impact of these discussions on products delivered?

- Are NSV holders reminded to seek travel advice when travelling overseas on either business or pleasure and then receiving the appropriate briefing, and where required debriefing? How is this reminder communicated?

- Is the expected culture and the ability to identify suspicious behaviours supported through a series of one-to-one challenges conducted by an Inspector on a random number of workforce personnel?

- Does the dutyholder have in place a procedure for when its workforce are carrying out activities under duress e.g. duress code? How is the duress code procedure communicated, and are those interviewed through the one-to-one challenges aware of the process?

- Are arrangements in place to ensure appropriate actions are taken on termination of employment?

7 FURTHER READING

7.1 Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403

7.2 Security Assessment Principles

7.3 Convention on the Physical Protection of Nuclear Material (CPPNM)

7.4 Nuclear Security Series 20 - IAEA Nuclear Security Fundamentals

7.5 IAEA Nuclear Security Series NO 7 – Nuclear Security Culture

7.6 IAEA Nuclear Security Series NO 8 – Preventative and Protective Measures against Insider Threats

7.7 HMG Security Policy Framework.

7.8 NISR 2003 Classification Policy

7.9 HMG Baseline Personnel Security Standard – Guidance on the Pre-Employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors

7.10 HMG Personnel Security Controls

7.11 Centre for The Protection of National Infrastructure - Personnel Security References

7.12 INFCIRC/225 IAEA – The Physical Protection of Nuclear Material

7.13 Cabinet Office SPF Personnel Security Supplement, Version 6.4, Dated November 2015.

7.14 HMG Maintaining Security Clearances – A Guide for Line Managers or Supervisors of Staff

7.15 Centre for the Protection of National Infrastructure – Personnel Security in Remote Working - A Good Practice Guide

7.16 ONR Inspection Guide – ONR-INSP-GD-064. General Inspection Guide

7.17 ONR Inspection Guide – ONR-INSP-GD-059. Guidance for Intervention Planning and Reporting.