|  |
| --- |
|  |
| ONR Technical Assessment Guide  Cooperation of Departments with Responsibility for Delivering Vetting and Ongoing Personnel Security Arrangements |



ONR Technical Assessment Guide (TAG)

Cooperation of Departments with Responsibility for Delivering Vetting and Ongoing Personnel Security Arrangements

**Professional Lead**: Protective Security

**Authored by**: Principal Inspector

**Approved by**: Superintending Inspector

**Issue No**.: 2

**Publication Date**: March 2024

**Next Major Review Date**: March 2029

**Doc. Ref**.: CNS-TAST-GD-8.1

**Record Ref. No**.: 2019/135717

Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 1 | New document |
| 2 | Inclusion of the role of relevant persons to the responsible person, updating links to guidance, and amendments reflecting changes in national security vetting processes. |

Contents

[1. Introduction 4](#_Toc160782773)

[2. Purpose and Scope 4](#_Toc160782774)

[3. Relationship to Licence and other Relevant Legislation 5](#_Toc160782775)

[4. Relationship to IAEA Security Standards and Guides 7](#_Toc160782776)

[5. Advice to Inspectors 8](#_Toc160782777)

[6. Regulatory Expectation 10](#_Toc160782778)

[7. Arrangements for Cooperation Between Departments 11](#_Toc160782779)

[8. Limitations 15](#_Toc160782780)

[References 16](#_Toc160782781)

[Glossary and Abbreviations 18](#_Toc160782782)

[Appendix 1: Extract of NISR 2003 Concerning Workforce Trustworthiness 19](#_Toc160782783)

# Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work and when making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.
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. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 (‘NISR 2003’) [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] 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 TAG is such a guide.

# Purpose and Scope

1. This TAG contains guidance to advise and inform ONR inspectors in the exercise of their regulatory judgment during intervention activities relating to the assessment of dutyholder’s processes for ensuring that departments with responsibility for delivering the Baseline Personnel Security Standard (BPSS), National Security Vetting (NSV) and Ongoing Personnel Security arrangements for its employees and contractors, which includes visitors, cooperate and work effectively in conjunction with one another.
2. The TAG aims to provide general advice and guidance to ONR inspectors on how to assess this aspect of a dutyholder’s security arrangements. It does not set out how ONR regulates the dutyholder’s arrangements. Neither does it prescribe the detail, or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate.

# Relationship to Licence and other Relevant Legislation

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.
2. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR 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 CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.
3. Regulations 9, 17(3) and 22(7) (d) of NISR relate to workforce trustworthiness and have been included at [Appendix 1](#_Appendix_1:_Extract) to this TAG. Furthermore, due consideration in relation to the treatment, use and the holding of personal information must also consider the following legislation:
4. General Data Protection Regulation 2016/679
5. Data Protection Act 2018
6. Human Rights Act 1998

iv) Rehabilitation of Offenders Act 1974

v) Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

vi) Rehabilitation of Offenders (Exclusions and Exceptions) (Scotland) Order 2003

vii) Rehabilitation of Offenders (Northern Ireland) Order 1978

viii) Equality Act 2010

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, associated guidance and policy documentation.
2. The Government Functional Standard on Security [3] is supplemented by the Cabinet Office OFFICIAL-SENSITIVE Personnel Security Policy (PSP) document [4] and associated Guidance on the Pre-employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors [5] which details arrangements on the Baseline Personnel Security Standard (BPSS) . Both supplements are identified as relevant good practice. They describe 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 GFS and PSP have been incorporated within the SyAPs.
3. 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.
4. The Government Security Classifications document, together with the ONR Classification Policy [6] describes types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

# Relationship to IAEA Security Standards and Guides

1. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [7] and the International Atomic Energy Agency (IAEA) Nuclear Security Fundamentals [8]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.
2. Fundamental Principle F of the CPPNM refers to security culture and states that all organisations should give due priority to the security culture and 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.
3. A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13 [9]. Further detail at the operational level is contained in an Implementing Guide on Preventive and Protective Measures against Insider Threats [10], in particular Sections 3 and 5. An Implementing Guide on Nuclear Security Culture [11] contains further information on establishing workforce trustworthiness (Section 4.3(i)).

# Advice to Inspectors

**National Policy and Guidance Related to Co-operation of Departments**

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.
2. **HMG** **Policy Expectations**. The Statement of HMG Personnel Security and NSV Policy [12] 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, criminal records (both spent and [at NSV] unspent as defined by the Rehabilitation of Offenders Act)) …[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 Human Resources (HR) and Occupational Health (OH), to work effectively together with the Security Department.

1. The guidance [12] further advises that:

“…security clearances may be refused or withdrawn where…personal circumstances, current or past conduct indicate that an individual may 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 individual at the time the process is carried out, but active, ongoing personnel security management is required to ensure that a security clearance remains valid. As a minimum, this will involve active consideration of the individual’s continuing conduct in respect of security matters;…”.

A dutyholder’s consideration of a subject’s continuing conduct is most effective when relevant departments work cooperatively.

1. **HMG BPSS Guidance**. BPSS guidance [5] 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 Pre-Employment Screening and National Security Vetting [13] gives a detailed explanation of the definition of staff (or employees) and contractors.

1. **NSV Questionnaires**.Information requested in the NSV questionnaires, which will vary according to the level of clearance relating to:

i) personal details

ii) medical conditions;

iii) the misuse of alcohol/ drugs or addictions;

iv) finances;

1. internet use;

vi) criminality;

vii) security behaviours; and

viii) the sponsor conducting the departmental/company record check;

indicates the broad range of information that dutyholders should consider in respect of ongoing personnel security and, it establishes the need for the work of relevant departments, including within the supply chain, to be properly integrated.

# 

# Regulatory Expectation

1. 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 to maintain a trustworthy workforce and minimising the possibility of insiders becoming a threat to nuclear security.

|  |  |  |
| --- | --- | --- |
| **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). | | |

# Arrangements for Cooperation Between Departments

1. Inspectors should consider that personnel security controls are effective only when there is close cooperation between the human resources, occupational health, and security departments. In light of this, three aspects are considered fundamental if dutyholders are to demonstrate adequate cooperation between such departments and these are detailed below:
2. There should be a formal mechanism for the onward reporting of incidents or concerns that identify a potential trustworthiness issue or which cause doubt as to the ongoing suitability of an individual to hold a clearance.
3. There should be a formal mechanism for tracking incidents or concerns raise through to their conclusion.

iii) Relevant personnel from Security, HR and OH should be suitably informed by appropriate training and guidance. This could, for example, include NPSA tool kits and published guidance available through the NPSA website [14] and training opportunities delivered through Counter Terrorism Security Advisers (CTSA).

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

i) 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 communicated effectively to, and understood by, the workforce.

ii) Management structures and procedures should have corporate oversight of, and provide for effective personnel security relationships between, the dutyholder security department and contractor organisations.

iii) There should be 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. Once an NSV clearance has been sponsored, reports to ONR should be made through the Aftercare Incident Reporting (AIR) portal on NSVS. All reports are to include details of any employment action being taken by the employer and/or contracting authority and how any risks identified are being managed. There may also be a legal reporting requirement directly to ONR under NISR 2003 Regulations 10,18 and 22 dependent on the nature of any actual, attempted or suspected incident.

iv) On sponsoring an initial or renewal NSV application, potential concerns should be established through the Departmental/Company Record Check. If concerns arise, but the sponsor still wishes to sponsor the application, these are to be recorded in the items of security interest section of the Security Questionnaire. For transfers or share requests, any concerns raised through the employers or contracting authorities’ standard pre-employment/appointment checks should provide an opportunity to establish any concerns before sponsoring the transfer or share request. Sponsors may wish to adapt the Departmental/Contractor Record Check process to use as a check prior to sponsoring a share or transfer of a clearance.

v) There should be evidence of engagements, meetings and processes which allow the Security, HR and OH departments to discuss and manage personnel security concerns and review the security culture and personnel security awareness and arrangements. At times, this will also include evidence of engagement with other departments to ensure appropriate security behaviours are addressed; for example, through induction arrangements, the use of official equipment and return of branded workwear, the formulation of training and/or learning and development products that contain personnel security messages.

vi) There should be evidence of inclusion of the security department as a stakeholder in formulating guidance and training associated with individual, managerial, and supervisory responsibilities; thereby ensuring any security considerations are appropriately considered.

vii) Where personnel security considerations exist, there should be evidence that the security department is a stakeholder involved in formulating and publicising relevant policies. This could include job advertisements and/or offer letters that include clearance requirements; policies relating to the use of social media; reporting hotlines/official whistleblowing arrangements; equal opportunities; harassment and bullying; employee assistance programme and drug and alcohol misuse.

viii) There should be arrangements to ensure relevant parties are aware of mandated reporting requirements, such as a positive drug/alcohol test, or other changes covered within the Change of Personal Circumstances questionnaires [15] (change in relationship status, nationality, criminality, significant financial difficulty where there is a mandated requirement to report such changes).

ix) Where relevant, there should be evidence of 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.

x) There should be evidence that arrangements exist for sharing, between relevant departments and line managers, the details of caveats and/or recommended conditions of employment for relevant individuals’ clearances; especially where they require ongoing management.

xi) There should be evidence that the department responsible for site visits notifies the security department in sufficient time to ensure clearances can be validated with UK or international partners.

Inspectors should consider:

a) Whether there is sufficient evidence of directorate/board level governance and oversight of cooperation between dutyholder departments with responsibility for personnel security; including, where appropriate, the supply chain?

b) Whether the dutyholder possesses relevant internal assurance policies and processes to evidence the above?

c) What evidence there is of cooperation, and how have relevant departments influenced one another?

d) What protocols exist between relevant departments?

e) Whether staff who occupy roles with responsibility for personnel security are suitably qualified and experienced; and whether the requirements for relevant training courses have been formally identified and demonstrably completed?

f) Whether relevant departments, including those within the supply chain, are aware of sources of guidance supporting an effective ongoing personnel security culture?

g) Whether recruitment, training/learning and development, conditions of service and exit policies/guidance/procedures support a dutyholder’s coordinated approach to personnel security?

h) Whether tender and contract award terms give sufficient weight to integrated personnel security procedures, policies and expectations?

i) Whether line managers are properly informed and trained on ongoing personnel security arrangements?

j) Whether the security department is provided with sufficient advance notice of site visits?

# 

# Limitations

1. The Data Protection Act 2018 and common law, under the law of confidence, contain obligations about patient confidentiality, which apply to doctors and others dealing with medical issues. 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 (see [16] and [17]). In some cases, this could justifiably limit the extent to which the work of different departments may be integrated. However, in making such an assessment, occupational health departments will be aware that, under the Nuclear Industries Security Regulations 2003 Regulations 9, 17 and 22 (See Appendix 1 for regulations in full), occupational health personnel are “relevant personnel” (as is the workforce generally) by having a duty to -

* Regulation 4 - the “responsible person” in ensuring the security of premises and the material, equipment and information.
* Regulation 17 - the “approved carrier” in ensuring the security of the material, information and premises.
* Regulation 22 – “any person[[1]](#footnote-2)” in ensuring the security of any sensitive nuclear information, uranium enrichment equipment or software within the possession or control of the person.

# References

|  |  |
| --- | --- |
| [1] | H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003. |
| [2] | ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry” [Online]. Available https://www.onr.org.uk/syaps/security-assessment-principles.pdf |
| [3] | H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://www.gov.uk/government/publications/government-functional-standard-govs-007-security |
| [4] | H.M. Government, OFFICIAL-SENSITIVE Personnel Security Policy |
| [5] | H.M. Government, “HMG Baseline Personnel Security Standard,” May 2018. [Online]. Available: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard |
| [6] | ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civil Nuclear Industry”. [Online]. Available https://www.onr.org.uk/documents/classification-policy.pdf |
| [7] | IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”. [Online]. Available: <https://www.iaea.org/publications/documents/conventions/convention-physical-protection-nuclear-material> |
| [8] | IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.[Online]. Available https://www.iaea.org/publications/10353/objective-and-essential-elements-of-a-states-nuclear-security-regime |
| [9] | IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011. [Online]. Available https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481\_web.pdf |
| [10] | IAEA, “Nuclear Security Series No. 8-G (Rev 1)- Preventive and Protective Measures against Insider Threats” [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858\_web.pdf |
| [11] | IAEA, “Nuclear Security Series No. 7 - Nuclear Security Culture,” 2008. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1347\_web.pdf |
| [12] | H.M. Government, “HMG Personnel Security Controls,” January 2022. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/1043588/HMG-Personnel-Security-Controls-V5-January-2022.pdf |
| [13] | ONR, “TAG-8.2 - Pre-employment Screening and National Security Vetting”.[Online]. Available: https://www.onr.org.uk/operational/tech\_asst\_guides/index.htm |
|  |  |
|  |  |
| [14]  [15] | NPSA, “Personnel & People Security,” August 2021. [Online]. Available: https://www.npsa.gov.uk/personnel-and-people-security  H.M Government "Change in Personal Circumstances" [Online]. Available: https://www.gov.uk/government/publications/change-of-personal-circumstances |
| [16] | GMC, “Confidentiality: Good practice in handling patient information,” January 2017. [Online]. Available: https://www.gmc-uk.org/-/media/documents/gmc-guidance-for-doctors---confidentiality-good-practice-in-handling-patient-information----70080105.pdf |
| [17] | NMC, “The Code: Professional standards of practice and behaviours for nurses, midwives and nursing associaties,” January 2015. [Online]. Available: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf |

|  |  |
| --- | --- |
|  |  |

# Glossary and Abbreviations

|  |  |
| --- | --- |
| AIR | Aftercare Incident Report |
| BPSS | Baseline Personnel Security Standard |
| CPPNM | Convention on the Physical Protection of Nuclear Material |
| CS&IA | Cyber Security and Information Assurance |
| FSyP | Fundamental Security Principle |
| GSS | Government Security Series |
| HR | Human Resources |
| IAEA | International Atomic Energy Agency |
| NISR | Nuclear Industries Security Regulations |
| NPSA | National Protective Security Authority |
| NSS | Nuclear Security Series |
| NSV | National Security Vetting |
| NSVS | National Security Vetting Solution |
| NSyP | Nuclear Security Policy |
| OH | Occupational Health |
| ONR | Office for Nuclear Regulation |
| PSP | Personnel Security Policy |
| SNI | Sensitive Nuclear Information |
| SyAP | Security Assessment Principle |
| SyDP | Security Delivery Principle |
| TAG | Technical Assessment Guide |
| UKSV | United Kingdom Security Vetting |

# 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 -

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

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-

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

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-

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

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.

1. In this context, “any person” means the body corporate that has possession or control of sensitive nuclear information, uranium enrichment equipment or uranium enrichment software in the United Kingdom. [↑](#footnote-ref-2)