|  |
| --- |
|  |
| ONR Technical Inspection Guide (TIG)  Nuclear Security Inspections |



ONR Technical Inspection Guide (TIG)

Nuclear Security Inspections

Authored by - Deputy Professional Lead (Protective Security)

Approved by - Professional Lead (Protective Security)

Approved by - Professional Lead (Cyber Security)

Issue No.: 1

Publication Date: Aug-23

Next Major Review Date: Aug-26

Doc. Ref.: CNS-INSP-GD-001

Record Ref. No.: 2023/44672

Table - Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 1 | Initial issue of integrated Nuclear Security TIG |

Contents

[1. Introduction 4](#_Toc143174304)

[1.1. Purpose 4](#_Toc143174305)

[1.2. Scope and Applicability 5](#_Toc143174306)

[1.3. Definitions 6](#_Toc143174307)

[2. Purpose of Security Inspections 7](#_Toc143174308)

[3. Guidance on NISR 2003 compliance 9](#_Toc143174309)

[4. Guidance on inspection of SPA and their implementation 9](#_Toc143174310)

[4.1. Guidance on selecting and scoping SPA to inspect 10](#_Toc143174311)

[4.2. Guidance on inspection delivery 12](#_Toc143174312)

[4.3. Guidance on inspecting strategic enablers 13](#_Toc143174313)

[4.4. Chief Nuclear Inspector Themed Inspections 14](#_Toc143174314)

[5. References 15](#_Toc143174315)

[Appendix A – Supply Chain / Regulation 22 16](#_Toc143174316)

# Introduction

1. The Nuclear Industries Security Regulations (NISR) 2003 (Ref. [1]) requires responsible persons to ensure the security of the nuclear premises, Nuclear Material (NM) or Other Radioactive Material (ORM) stored on the premises. NISR 2003 also places legal requirements on holders of Sensitive Nuclear Information (SNI) and on carriers transporting Category I - III NM.
2. The Office for Nuclear Regulation (ONR) has established a set of outcome-focused Security Assessment Principles (SyAPs) (Ref. [2]) which provides a framework to assess security arrangements defined in each security plan (SP) and enables the inspector to make consistent regulatory judgements on the adequacy of those arrangements.
3. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are outcome-focused and do not prescribe what a dutyholder’s SP should contain. Dutyholders are responsible for designing, implementing, and assuring the efficacy of their security arrangements. The dutyholder submits its SP to ONR for approval; once an SP has been approved, ONR conducts regular inspections to judge dutyholder compliance with their approved SP (and thus with NISR 2003).

## Purpose

1. Regulating under NISR 2003 (Ref [1]) entails a two-stage approach and there is a suite of supporting ONR guidance documentation:

* Technical Assessment Guides (TAGs) assist inspectors in assessing and judging the adequacy of standards, procedures and arrangements (SPA) described in a dutyholder’s SP.
* Once an SP has been approved by ONR, this Technical Inspection Guide (TIG) assists inspectors in judging compliance against the approved SP.

1. The purpose of this TIG is to facilitate a consistent and effective approach to inspecting compliance with SPA described in an approved SP. It is applicable across the Nuclear Security purpose and therefore covers both Protective Security and Cyber Security and Information Assurance, as well as their sub-specialisms.

## Scope and Applicability

1. This TIG is applicable to all ONR security specialisms and sub-specialisms:

* Cyber Security and Information Assurance
  + Cyber Security
  + Information Assurance
  + Supply Chain
* Protective Security
  + Physical Security
  + Transport Security
  + Personnel Security

1. The term “standards, procedures and arrangements” (SPA) is used extensively throughout NISR 2003 in reference to nuclear premises, approved carriers, and holders of SNI. Full explanations and application can be found in NISR 2003 (Ref [1]).
2. The judgements made by the inspector will relate primarily to implementation of SPA described in the SP, to ensure that the written claims, arguments and evidence (CAE) are fully demonstrated on the ground. This guide will assist in making consistent regulatory judgements and decisions.
3. Inspectors are reminded that an inspection may reasonably require review of the described SPA themselves (as distinct from their implementation). As ONR takes a sampling approach to regulation, it is possible that elements of an approved SP have not previously been assessed. It is also possible that a security situation may evolve over time. Therefore, when reviewing or inspecting evidence as part of a compliance inspection, inspectors may also form judgements on the adequacy of the SPA described in the approved SP.
4. Straightforward judgements might be addressable as part of the inspection, (for instance through updating supporting documentation referenced in the SP e.g. local working instructions) or through raising a regulatory issue. Alternatively, inspector observations can provide regulatory intelligence which assists in targeting future ONR assessment activity*.* SyAPs (Regulatory Assessment of Security Plans (RASyP) 7 – Security Plan Maintenance) advises that an SP should be actively maintained and reviewed regularly, and dutyholders should welcome regulatory input in the interests of continuous improvement.
5. This TIG 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.

## Definitions

1. Within this document, the term security plan (SP) refers primarily to site security plans required under NISR 2003 (Ref [1]) Regulation 4, and Transport Security Statements (TSS) required under Regulation 16. It may also apply to written cyber security and information assurance arrangements adopted by Regulation 22 dutyholders.
2. The term standards, procedures and arrangements (SPA) refers to the totality of a SP, including SPA explicitly detailed within, relied upon, or referenced by, the plan. For example (not exhaustive) it can be interpreted to cover:

* any Security System, Structure or Component (SySSC) such as an intrusion detection system, IT network firewall, or security camera etc.
* any Task Important to Nuclear Security (TINS) such as the conduct of vetting checks, IT network monitoring, or conduct of searching etc.
* any standard such as a social media policy, homeworking policy etc.

1. The term ‘dutyholder’ 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; approved carriers, as defined in NISR 2003; and those handling, storing and processing (or proposing to do so) SNI.

Table 1 – Table of Acronyms

| Term/Acronym | Description |
| --- | --- |
| CAE | Claims, Arguments and Evidence |
| FSyP | Fundamental Security Principles (under SyAPs) |
| KSyPP | Key Security Plan Principles (under SyAPs) |
| NISR 2003 | The Nuclear Industries Security Regulations 2003 |
| NM | Nuclear Material |
| ORM | Other Radioactive Material |
| RASyP | Regulatory Assessment of Security Plans (under SyAPs) |
| REDE | Regulator Evaluated Demonstration Exercises |
| SAPs | Safety Assessment Principles |
| SIS | Security Improvements Schedule |
| SNI | Sensitive Nuclear Information |
| SP | Security Plan |
| SPA | Standards, procedures and arrangements |
| SyAPs | Security Assessment Principles |
| SyDPs | Security Delivery Principles (under SyAPs) |
| SySSC | Security System, Structure or Component |
| TAG | Technical Assessment Guide |
| TIG | Technical Inspection Guide |
| TINS | Task Important to Nuclear Security |
| TSA | Temporary Security Arrangement |
| TSP | Temporary Security Plan |
| TSS | Transport Security Statement |

# Purpose of Security Inspections

1. The primary purpose of the inspection is to ensure compliance with the law. NISR 2003 (Ref [1]), Regulation 7 states that the responsible person in relation to each nuclear premises must comply with the SPA described in the approved SP for the premises. Similarly, Regulation 17 states that an approved carrier must comply with the SPA described in an approved TSS. This is the basis for the majority of ONR security inspections: ensuring the dutyholder is complying with the approved plan.
2. Whilst this principle holds true for the majority of ONR security activity, some specialist areas may deviate slightly and merit additional explanation:

* **Transport Security – Class B carriers.** NISR 2003 applies to all approved carriers, but ONR takes a proportionate approach in relation to the size and structure of carrier organisations and the category of NM they are approved to transport. Class B approved carriers based at UK civil licensed nuclear sites may incorporate transport security arrangements into their approved SP. For other Class B approved carriers, it will be sufficient that SPA described in the TSS comply with ‘Guidance for Class B Approved Carriers’ (Ref. [3]).
* **Personnel Security / Workforce Trustworthiness.** ONR ensures dutyholders’ workforce trustworthiness arrangements comply with His Majesty’s Government (HMG) Government Functional Standard GovS007: Security (Ref. [4]) and other underpinning documents (including the OFFICIAL-SENSITIVE Personnel Security Policy, HMG Personnel Security Controls, and UK Government guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors). Additional areas of mandated workforce trustworthiness compliance exist within ONR SyAPs, specifically annexes (OFFICIAL-SENSITIVE) relating to the mandated clearance levels to be applied, dutyholders’ signing authorities against the Baseline Personnel Security Standard, and visit arrangements. Such arrangements shall be contained within a nuclear site’s SP or an approved carrier’s transport security statement.
* **Supply Chain - Regulation 22 Dutyholders.** As Regulation 22 dutyholders are not required to produce an SP for approval, ONR has a different arrangement for gathering assurance regarding their securing of SNI and application of relevant good practice. This arrangement is detailed in Appendix A.
* **Regulator Evaluated Demonstration Exercises (REDE).** REDEs are a means by which a dutyholder must demonstrate that they can: implement effective and integrated emergency preparedness and response arrangements, for all credible events based upon the Design Basis Threat (DBT); achieve the required security outcomes, with the appropriate level of confidence; and effectively manage the consequences of such DBT events.

The scope of a REDE, its associated objectives and supporting scenario should be agreed by the inspection team. A REDE should be evaluated against specific areas and functions and associated performance statements.

It is for the inspection team to decide which areas and performance statements are relevant, taking account of the required security outcomes, the characteristics of the site, the challenges presented by the scenario and agreed objectives. The inspection team should not be beholden to, or constrained by, the exercise performance criteria established by the dutyholder. If a REDE is judged to be inadequate, then the inspection team must decide whether a full or partial re-demonstration is required. Further guidance on evaluating REDEs and associated relevant good practice is contained in the associated guidance document ‘Regulator Evaluated Demonstration Exercises – Aide Memoire for Inspectors’ (Ref [5]).

# Guidance on NISR 2003 compliance

1. NISR 2003 (Ref [1]), Regulation 4 sets out the need for an approved SP to be in place at all times which describes the SPA to ensure the security of the elements specified within this regulation and which are applicable to the dutyholder. It further describes a number of key aspects that require additional and specific consideration: pre-employment checks and national security vetting; movement of NM; equipment and software used in connection with activities involving nuclear material / ORM; policing and guarding, and contingency plans. Finally, it covers the consideration of threats posed to existing sites by plant and machinery being used during construction of an adjacent site.
2. **Nuclear premises:** Regulation 7 states that the responsible person in relation to each nuclear premises must comply with the SPA described in the approved SP for the premises. Regulation 9 states that specified personnel must have been assessed to be of suitable character and integrity.
3. **Transport security and approved carriers:** Regulation 17 states that an approved carrier must comply with the SPA described in an approved TSS. (See also paragraph 15 regarding Class B carriers.)
4. **Regulation of SNI, uranium enrichment equipment and software:** Regulation 22 sets out the need for those specified to maintain such security SPA as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within their possession or control. Details of how ONR determines whether or not the risk has been minimised are contained in Appendix A.
5. Full wording can be found in NISR 2003, and comprehensive guidance on interpretation of the law is provided in ONR publication ‘**Nuclear Industries Security Regulations 2003 - Guidance for Inspectors**’ (Ref. [6]).

# Guidance on inspection of SPA and their implementation

1. This TIG should be read in conjunction with existing ONR guidance on inspection activity, which is both detailed and comprehensive:

* **ONR-INSP-GD-059** (Guidance for Inspection Strategy Planning and Recording – Ref. [7]) covers the production of annual inspection plans, regulatory attention levels, resource allocation, the integrated intervention strategy, inspection types, and associated governance arrangements.
* **ONR-INSP-GD-064** (General Inspection Guide – Ref. [8]) covers the stages of the inspection process – Planning, Preparation, Delivery and Record. This guidance applies to all security compliance inspections, whether planned or reactive. It provides detailed advice on a variety of important topics such as use of the WIReD system, inspection ratings, Regulatory Issues and the Enforcement Management Model (EMM).

## Guidance on selecting and scoping SPA to inspect

1. Compliance inspections are an essential element of ONR's overall intervention strategy on nuclear premises. These are intended to establish that the arrangements within the SP have been effectively implemented, such that they are fit for purpose and will fulfil their security functional requirements, in support of achieving the required security outcome.
2. Whilst it is recognised that all nuclear premises are required by law to have an approved SP, there will be considerable variation between, for example, SPA for an operational reactor site versus a site holding only Cat IV material and undergoing decommissioning. ONR is a sampling organisation and it would not be appropriate to inspect every aspect of SPA compliance with all aspects of every SP.
3. The purpose and principles of enforcement, as set out in the ONR Enforcement Policy Statement (ref. [9]), should be at the forefront of an inspector’s mind when undertaking all stages of compliance inspection. In particular, security inspectors should ensure that inspections are targeted according to relevant factors such as regulatory attention level, regulatory strategy, level of risk, and regulatory intelligence.
4. Through interrogation of CAE in the approved SP, inspectors will be able to identify appropriate SPA, their intended function, and the contribution they make towards meeting required security outcomes. Inspectors can then shape the inspection scope, to obtain assurance that SPA have been implemented in accordance with the approved SP and are achieving the necessary effect.
5. SyAPs broadly divides FSyPs into two categories: Strategic Enablers (FSyPs 1-5) and Secure Operations (FSyPs 6-10). Many compliance inspections will include the sampling of selected elements from FSyPs 6-10 (depending on security specialism), which focus upon the operational implementation and maintenance of nuclear security:

* **FSyP 6: Physical Protection Systems**[[1]](#footnote-2) (Categorisation for Theft; Categorisation for Sabotage; Physical Protection System Design; Vulnerability Assessments; Adjacent or Enclave Nuclear Premises; Nuclear Construction Sites; Protection of Nuclear Material During Offsite Transportation).
* **FSyP 7: Cyber Security and Information Assurance** (Effective Cyber and Information Risk Management; Information Security; Protection of Nuclear Technology and Operations; Physical Protection of Information; Preparation for and Response to Cyber Security Incidents).
* **FSyP 8 - Workforce Trustworthiness** (Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security; Pre-employment Screening and National Security Vetting; Ongoing Personnel Security).
* **FSyP 9 - Policing and Guarding**1(CNC Response Force; Local Police Operations in Support of the Dutyholder; Security Guard Services).
* **FSyP 10 - Emergency Preparedness and Response**1(Counter Terrorism Measures, Emergency Preparedness and Response Planning; Testing and Exercising the Security Response; Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event).

1. Inspectors should also consider the SyAPs Key Security Plan Principles (KSyPP), which ought to be applied across the breadth of an approved SP. Applying these principles requires judgement and proportionality, in deciding which are relevant to a situation and the adequacy of compliance:

* KSyPP 1: Secure by Design
* KSyPP 2: The Threat
* KSyPP 3: The Graded Approach
* KSyPP 4: Defence in Depth
* KSyPP 5: Security Functional Categorisation and Classification
* KSyPP 6: Managing Changes to Security SPA
* KSyPP 7: Codes and Standards

1. The process should also highlight likely resource requirements e.g. support from other ONR specialisms or purposes. Inspectors should consider an integrated approach, particularly when inspecting SyAPs strategic enablers (see Section 4.3). The level of resource support could vary, for example:

* Before inspecting backup power for security systems, the inspector might ask an ONR electrical engineering specialist to review SPA in the SP, and to provide advice on how the security inspector can verify compliance.
* To inspect SPA concerning human performance in a security control room, the security inspector might propose a full, joint inspection with an ONR Human Factors specialist.

1. During the preparation phase, it is often appropriate to obtain and review evidence from the dutyholder. Review of such evidence in advance may help focus the inspection and allow more time for targeted activity on site.
2. It is recommended that requirements for the delivery phase be clearly identified to the dutyholder in advance, to allow them to prepare effectively. The inspector should make the dutyholder aware of the staff and stakeholders that they will need to see as part of the inspection. More detailed guidance is contained in ONR-INSP-GD-064 (Ref [8]).
3. In addition to examining a specific theme or subject, certain activities may form a routine component of most security inspections. These might include:

* Meetings with key personnel or departments (e.g. internal regulator)
* Review of open Regulatory Issues
* Review of ongoing permissioning activities e.g. Temporary Security Plans (TSP) / Temporary Security Arrangements (TSA)
* Review of reportable incidents under NISR Regulations 10, 18 or 22
* Review of dutyholder records for incidents deemed non-reportable
* Review of Security Improvements Schedule (or equivalent) commitments

## Guidance on inspection delivery

1. Inspectors will inspect SPA as set out in the approved SP, review the implementation of those SPA, and judge whether the dutyholder is complying with the SPA described in the approved SP (NISR 2003, Regulation 7 (Ref [1]).
2. ONR requires inspectors to conduct compliance inspections in accordance with ONR guidance, policy and with an enabling approach (Ref. [10]) which satisfies the provisions of the Regulators Code (Ref. [11]). The inspector should apply the detailed guidance in the ‘General Inspection Guide’ ONR- INSP-GD-064 (Ref [8]). These documents explain a range of regulatory tools and approaches available to inspectors, from influence and persuasion through to formal enforcement. Evaluation of compliance is covered in detail under section 5 (Delivery) of ONR-INSP-GD-064.
3. One additional tool for security inspections is available under NISR 2003 (Ref [1]). Regulation 4.(2) states that an SP must describe the SPA “adopted or to be adopted…” (or for a TSS, Regulation 16.(2)). Measures *to be adopted* are recorded as a regulatory commitment in the dutyholder’s “Security Improvement Schedule” (or equivalent title), a key supporting document which forms part of the approved SP. It lists regulatory commitments with deadlines for delivery, against which dutyholders can be held to account under NISR 2003.
4. The inspector should adopt a proportionate and graded approach, utilising the history from previous interventions to inform their expectations. Inspectors should ensure that any issues identified in previous interventions have been followed up.

## Guidance on inspecting strategic enablers

1. This TIG covers security SPA including protective and physical security; emergency preparedness and response; workforce trustworthiness; and cyber security and information assurance. Whilst these form the core of security inspection activity, inspectors must also consider SyAPs strategic enablers, which overlap heavily with the other ONR purposes. SyAPs aligns closely with the Safety Assessment Principles (SAPs) and inspectors should consider a cross-purpose approach. Brief examples include:

* FSyP 1: Leadership and Management for Security
  + Responsibility, accountability and decision making
  + Learning from experience (e.g. security events, internal inspections)
  + Assurance processes to support internal assessment of performance
* FSyP 2: Organisational Culture
  + NS-INSP-GD-070 (Ref. [12]) identifies cultural “warning flags” e.g.:
    - Overconfidence, lack of healthy unease and drift in standards
    - Deviation from established arrangements
    - Impaired sharing and isolationism
* FSyP 3: Human Performance Management
  + Required numbers and competencies of personnel
  + Ergonomic design of workspaces, equipment and user interfaces
  + Procedures and administrative controls to minimise human error
* FSyP 4: Nuclear Supply Chain Management[[2]](#footnote-3)
  + Procurement by an intelligent customer
  + Screening and oversight of suppliers
  + Commissioning arrangements
* FSyP 5: Reliability and Resilience2
  + Detailed design specification covering reliability and resilience
  + Contingency to cover periods of maintenance or unserviceability
  + Records of examination, inspection, maintenance and testing

## Chief Nuclear Inspector Themed Inspections

1. Inspectors may be required to support Chief Nuclear Inspector (CNI) themed inspections. Introduced in 2017, these are designed to examine regulatory matters that are strategic or broader in nature than ONR’s more routine regulatory inspection activities. Previous themes have included climate change, and management of ageing facilities. Further details can be found in ONR-INSP-GD-059, Appendix 1D.

# References

|  |  |
| --- | --- |
| [1] | Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403. |
| [2] | ONR, Security Assessment Principles for the Civil Nuclear Industry, 2022. |
| [3] | ONR, CNSS-SEC-GD-001 - Nuclear Transport Security Guidance for Class B Approved Carriers. |
| [4] | HMG, Government Functional Standard GovS007: Security. |
| [5] | ONR, Regulator Evaluated Demonstration Exercises – Aide Memoire for Inspectors (CM9: 2023/39235). |
| [6] | ONR, CNSS-SEC-GD-002 - Nuclear Industries Security Regulations 2003 – Guidance for Inspectors. |
| [7] | ONR, ONR-INSP-GD-059 - Guidance For Inspection Strategy Planning and Recording. |
| [8] | ONR, ONR-INSP-GD-064 - General Inspection Guide. |
| [9] | ONR, Enforcement Policy Statement, 2021. |
| [10] | ONR, Holding Industry to account and influencing improvements in nuclear safety and security – Enabling Regulations in practice, 2018. |
| [11] | Department for Business Innovation and Skills, Regulators Code, 2014. |
| [12] | ONR, NS-INSP-GD-070 Organisational Culture Guide for Inspectors. |

# Appendix A – Supply Chain / Regulation 22

1. As Regulation 22 dutyholders are not required to produce a security plan for approval, ONR has a different arrangement for gathering assurance regarding their securing of SNI and application of relevant good practice.
2. In order for a Regulation 22 dutyholder to demonstrate evidence of effective arrangements, and noting that SNI always accompanies a Government Security Classification, ONR considers the expectations and requirements articulated within Government Functional Standard GovS007: Security to be relevant good practice. As such ONR have directly mapped 5 of the 10 Fundamental Security Principles (FSyP) from the SyAPs to GovS007 in order to provide a framework for dutyholders to evidence their arrangements and for regulators to make judgements on their adequacy. The relevant FSyPs are FSyP 1, 2, 3, 7 and 8. Other FSyPs are considered out of scope.
3. Those dutyholders complete an Inherent Risk Profile Questionnaire (IRPQ) to determine the level of inherent risk a particular facility or IT system holds. This is largely based upon the classification and quantities of SNI held at that facility or on that system. For Regulation 22 dutyholders with multiple facilities and systems, their corporate inherent risk profile level is calculated cumulatively, taking into account the SNI held across all their facilities and systems.
4. The calculated inherent risk profile levels are then used to determine the ‘evidencing expectations’[[3]](#footnote-4) that the dutyholder is required to demonstrate meeting, corporately and for each facility and system where SNI is handled. For most Regulation 22 dutyholders, the IRPQ and ‘evidencing expectations’ processes are completed on the List N portal and approved by the dutyholder’s Contracting Authority (CA), where appropriate.
5. ONR inspectors have access to the Regulation 22 dutyholders submissions and the CA’s verification, approval and ongoing assurance evidence via the List N portal. The availability of such evidence enables inspectors to carry out partial or wholly desk top based inspections.
6. ONR inspectors should carry out sample inspections of Regulation 22 dutyholders, to determine their compliance with NISR 2003 (Ref [1]). Generally, an inspection will focus on a particular facility or system, considering relevant supporting evidence from the ‘Corporate Evidencing Expectations’ submission. For larger Regulation 22 dutyholders, with multiple facilities and systems, an inspector may deem it appropriate to conduct a more corporate-focused intervention.
7. ONR has communicated the following parameters when undertaking Regulation 22 inspections:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | Inspection method | | |
| **Inherent Risk Profile Level** | **Maximum Inspection Frequency** | **Desktop Review of Evidence** | | **On Site Facility Inspection** |
| High | 2 years | Yes | | Yes |
| Moderate | 3 years | Yes | | Optional |
| Low | 4 years | Yes | | Optional |
| Very Low | 5 years | Yes | | No |

1. It should be noted that the parameters detailed above may be overridden, according to the inspector’s judgement, based upon factors that may affect risk to SNI, such as dutyholder breaches, poor provision of evidence or engagement with ONR, company acquisitions and mergers etc.
2. Due to the high number of Regulation 22 dutyholders, organisations, facilities and systems should be selected for inspection using a risk informed approach. Factors such as inspection history, incident history, number of Contracting Authorities, experience handling SNI and other factors will be taken into consideration, alongside the inherent risk profile, when developing the intervention plan. This will ensure that the impact of regulation to any particular dutyholder is applied proportionately.
3. In light of the relatively infrequent nature of Regulation 22 inspections for many dutyholders, ONR inspectors should aim to gather assurance across all five of the relevant FSyPs, during a single inspection. Specific evidence expectations should be selected, to provide an indicative level of compliance against each FSyP. As such, inspections may be broader and shallower than those conducted at nuclear premises, though inspectors retain the ability to drill down into potential issues identified during an inspection. As such, there may be times when it is not feasible to sample each FSyP due to issues encountered during an inspection.
4. It should be noted that Personnel Security arrangements can differ amongst Regulation 22 dutyholders. Inspectors may consider the following when inspecting such arrangements.
5. Personnel security arrangements for Regulation 22 organisations that are not sponsors of national security vetting clearances in the civil nuclear industry, are to meet expected standards as detailed within the Security Aspects Letters (SAL) agreed with the Contracting Authority. The contracting authority is expected to ensure compliance with the SAL on an ongoing basis. Where these standards relate to achieving HMG Personnel Security Controls, including the submission of company record checks to support national security vetting applications, and aftercare reporting, these arrangements may be assessed by ONR Personnel Security Inspectors when the Contracting Authority is subject to a personnel security intervention.
6. ONR inspectors, when inspecting Regulation 22 dutyholders who are unable to sponsor civil nuclear national security vetting applications, will assess that the organisation’s personnel security culture has relevant policies in place which are publicised and adhered to. Such policies will include, and are not limited to, harassment and bullying, equal opportunities, use of social media, reporting hotlines/whistleblowing and drug and alcohol misuse. In reviewing these arrangements, ONR inspectors will look to establish that policies support an effective security culture, internal departments within the Regulation 22 organisation engage with each other on relevant matters, and that issues of a potential security concern are shared with an appropriate person in the Contracting Authority.

1. FSyPs 4, 5, 6, 9 and 10 are considered out of scope for Regulation 22 dutyholders. [↑](#footnote-ref-2)
2. FSyPs 4, 5, 6, 9 and 10 are considered out of scope for Regulation 22 dutyholders. [↑](#footnote-ref-3)
3. The evidencing expectations are based on five FSyPs that are applicable to Regulation 22, and the relevant underpinning TAGs. To find out more, refer to the List N webpage (www.onr.org.uk/listn) [↑](#footnote-ref-4)