|  |
| --- |
|  |
| ONR Technical Assessment Guide  Information Security |



ONR Technical Assessment Guide (TAG)

Information Security

Authored by: Inspector, Cyber Security and Information Assurance

Approved by: Superintending Inspector

Professional Lead: Cyber Security and Information Assurance

Issue No.: 2.1

Publication Date: Aug-23

Next Major Review Date: Mar-27

Doc. Ref.: CNS-TAST-GD-7.2

Record Ref. No.: 2019/135702

Table - Revision commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 2 | Revisions to RGP from HMG, ONR and the National Technical Authority and alignment ONR Style Guide. |
| 2.1 | Minor update to incorporate references to newly published NISR question sets as well as minor formatting updates. |

Contents

[1. Introduction 4](#_Toc142391154)

[2. Purpose and Scope 4](#_Toc142391155)

[3. Relationship to Licence and other Relevant Legislation 4](#_Toc142391156)

[4. Relationship to Security Assessment Principles and IAEA Security Standards and Guides 5](#_Toc142391157)

[5. Advice to Inspectors 7](#_Toc142391158)

[References 21](#_Toc142391159)

[Glossary and Abbreviations 23](#_Toc142391160)

[Appendix 1 – Concentration of Risk 24](#_Toc142391161)

# Introduction

1. The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) [1]. This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 [2].
2. The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

# Purpose and Scope

1. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgement during assessment activities relating to a dutyholders arrangements to protect information. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholders arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail 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 minimise the risk to their holdings of SNI.   
   ONR considers CS&IA to be an important component of a dutyholders arrangements in demonstrating compliance with relevant legislation.
3. The HMG Government Functional Standard on Security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management.   
   It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within the Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not. Note that this standard replaces the HMG Security Policy Framework (SPF) [4]; however, the policies which sit within the SPF, which was updated in December 2022, remain in effect but are now in support of the HMG Government Functional Standard [3].
4. The HMG Government Security Classifications (GSC) [5] document, together with the NISR 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 Security Assessment Principles and IAEA Security Standards and Guides

1. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholders security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholders submission demonstrating they have effective processes in place to achieve SyDP 7.2 – Information Security, in support of FSyP 7 – Cyber Security & Information Assurance. This TAG is consistent with other TAGs and associated guidance and policy documentation.
2. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [7] whilst IAEA's Nuclear Security Series (NSS) [8] provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security.
3. Fundamental Principle L of the CPPNM refers to confidentiality and details that the ‘State should establish requirements for protecting the confidentiality of information, the unauthorised disclosure of which could compromise the physical protection of nuclear material and nuclear facilities’. The importance of issues relating to CS&IA is also recognised in the Nuclear Security Fundamentals [9], specifically:

* Essential Element 3: Legislative and Regulatory Framework – 3.3   
  The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime:
  + g) Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.
  + h) Ensure that prime responsibility for the security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets rests with the authorised persons.
* Essential Element 12: Sustaining a Nuclear Security Regime – 3.12   
  A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:
  + h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

1. A more detailed description of the elements is provided in NSS Nuclear Security Recommendations level guidance, specifically NSS 13 [10], paragraphs 3.53 to 3.55 explicitly refer to issues relating to confidentiality. Implementing Guide NSS No. 23-G ‘Security of Nuclear Information’ [11] ‘provides guidance on implementing the principle of confidentiality and on the broader aspects of information security (i.e. integrity and availability)’, and Technical Guidance NSS No. 17 ‘Computer Security at Nuclear Facilities’ [12] ‘provides guidance on how to establish or improve, develop, implement, maintain, and sustain computer security within nuclear facilities to establish computer security measures that protect sensitive digital assets … from the consequence of cyber-attacks’.

# Advice to Inspectors

1. The security of information is essential to maintain civil nuclear operations and ensure public confidence. Therefore, to operate effectively, the civil nuclear industry should maintain the confidentiality, integrity and availability of its SNI[[1]](#footnote-2).
2. SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise data in various formats (such as digital, hard copy and knowledge) as well as information technology (IT) and operational technology (OT) (equipment or software). It is a dutyholders responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI, computer-based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilised on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should always be considered.
3. Whilst not taking precedent over the legal definitions highlighted in the NISR Classification Policy [6], a simple working definition of SNI can be described as information relating to activities carried out on or in relation to civil nuclear premises; and of value to an adversary planning a malicious act[[2]](#footnote-3). It includes information which requires a classification in accordance with the NISR Classification Policy. The NISR Classification Policy uses the principles and classifications detailed in the HMG GSC System [5]. The NISR Classification Policy provides descriptions of consequences relating to the nuclear industry that should form part of the basis of judgement when applying a security classification to a specific document. Specific examples for different types of documents and data that may contain SNI are provided in the Classification Guidance at Annex A to the NISR Classification Policy.
4. Information and associated assets may be held by personnel of dutyholders, and their supply chain companies (and/or if SNI is shared with customer/peer organisations), and effective CS&IA arrangements should always address the protection of these assets and in all forms. Information security includes management of classified contracts involving SNI and encompasses all relevant aspects including:

* Information Assurance (IA) strategy, policy and standards
* Data classifications and sensitivities
* Identification of classified contracts
* CS&IA assessments of third party suppliers
* Assurance of third party suppliers
* End of contract

1. This TAG draws heavily on Relevant Good Practice (RGP) provided by National Cyber Security Centre (NCSC) as the National Technical Authority (NTA) for information assurance. Other sources of RGP which support the protection of information includes, but is not limited to, international standards such as International Organisation for Standardisation/ International Electrotechnical Commission (ISO/IEC) 27001 [13] and International Society of Automation (ISA) ISA/IEC 62443 [14], the Information Security Forum (ISF) Standard of Good Practice for Information Security, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework [15]. Advice and guidance on a risk assessment approach and methodology, the protection of IT and OT, and the physical protection of information can be found in TAGs 7.1: Effective Cyber and Information Risk Management [16], 7.3: Protection of Nuclear Technology and Operations [17], and 7.4: Physical Protection of Information [18], respectively.

## Regulatory Expectations

1. The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their approach to the protection of information in support of maintaining effective CS&IA arrangements.

|  |  |  |
| --- | --- | --- |
| FSyP 7 - Cyber Security and Information Assurance | Information Security | SyDP 7.2 |
| Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets | | |

## Information Assurance Strategy, Policy and Standards

### Information Assurance Strategy

1. Dutyholders should ensure that the organisation has a coherent strategy to implement CS&IA in all relevant areas of the business. The scope of the strategy should be the same as that of the risk assessment carried out as part of the defined risk management process in TAG 7.1 [16].
2. The scope should include partners, customers, service providers and suppliers holding information and associated assets for which the organisation is responsible. The requirements for third parties should be embodied in contracts along with consequences for non-compliance so that they are enforceable.
3. The strategy should be formally endorsed by the Board and overseen by a member responsible for cyber and information risk management. It should be delivered under a governance structure that defines those roles that ensure it is implemented effectively.
4. A specific programme for CS&IA (or a similar mechanism) should be considered to facilitate delivery of the strategy. The programme should have clear aims and those delivering it should be accountable under governance and reporting arrangements. The scope of the CS&IA programme should be the same as that of the CS&IA strategy with clear line of sight between the two, and with adequate resourcing and support from a communications plan to explain its purpose across the organisation (to include third parties).

### CS&IA Policy and Standards

1. The CS&IA strategy and its associated programme should be underpinned by a comprehensive policy structure that is tailored to the organisation.   
   The policy should be achievable, enforceable and auditable. The topics within the policy should include, but not be limited to, the following:

* Organisational structure
* Information asset identification and management
* Risk assessment, treatment and management
* Records retention
* Physical and environmental management
* Personnel security & management
* System security design
* Computer and network security
* Operational procedures
* Social engineering
* Acceptable system use
* Security training
* Third party management
* Incident management
* Business Continuity and Disaster Recovery (including pandemic response)
* Remote/home working practices
* Identification and handling of SNI

1. Technical CS&IA policy measures are described in more detail in   
   TAG-7.3 [17]. Further guidance on CS&IA policy aspects is available from a number of sources including:

* HMG (e.g. Centre for the Protection of National Infrastructure (CPNI), NCSC, Cabinet Office)
* Nuclear authorities (e.g. ONR, IAEA, IEC, other regulators including the US Nuclear Regulatory Commission and Canadian Nuclear Safety Commission)
* International Bodies (e.g. IEC, NIST, ISACA, SANS, ISF)

### Inspectors should consider:

* Does the dutyholder have a CS&IA strategy in place that is appropriate to the organisation?
* Does the information assurance strategy state how it will align to the organisation’s strategic objectives? Can they provide evidence the two are integrated? Consider how business objectives are aligned to IT and security objectives.
* Is the strategy adequate to identify and manage risks to information and associated assets?
* Is the strategy underpinned by a timely and appropriately resourced programme to deliver it?
* Does the dutyholder have a CS&IA policy in place that is scoped to the organisation?
  + Is there a documented policy which is used to drive the dutyholders information strategy?
  + How is the policy made to be achievable, enforceable and auditable?
  + What areas of the organisation does the policy cover?
  + Are all relevant topics adequately addressed?
  + Within the policy, is there reference to standards to demonstrate relevant good practice? (e.g. HMG, Nuclear Authorities, International Bodies)?

## Data Classification and Sensitivities

1. It is imperative that dutyholders should have a clear understanding of information and associated assets for which they have responsibility. This is reinforced in the qualifying text in SyAPs under SyDP 7.2, which states that dutyholders should establish mechanisms and processes within their organisation to ensure assets are properly classified in accordance with all relevant classification policy.
2. Information and associated assets should be ascribed a value and an owner.   
   This latter element is crucial because effective cyber and information risk management relies upon understanding of the value of assets and responsibility for ensuring that they are protected adequately.
3. Annexes F and G to the SyAPs provide a framework for categorising SNI (including IT used for processing, storage or transmission) and equipment or software (used in connection with activities involving nuclear material and other radioactive material), with which a dutyholders classification mechanisms and processes should fit within.
4. Dutyholders should create, maintain and appropriately protect an Information Asset Register (IAR) or similar mechanism that is an accurate record of what SNI and associated assets the organisation is responsible for, what format they are in, what value they have and where they are located.
5. Dutyholders should consider the use of electronic data labelling or tagging tools to mark and track information and associated assets using metadata.
6. The scope of the IAR should include SNI and associated assets managed by third party suppliers. In some circumstances this can be accomplished by a contractual obligation for them to maintain their own IAR. It should be subject to maintenance and review on a regular basis to confirm that its contents are accurate.
7. Dutyholders should create and maintain a specific register for holdings of above OFFICIAL-SENSITIVE SNI (including legacy documents classified CONFIDENTIAL where appropriate). Appropriate document control and accounting should accurately reflect:

* What SNI information and associated assets the organisation is responsible for, what format they are in, and what classification they are.
* Where they are located (final and temporary disposal). Details of who the responsible and supervisor officers are for the register upkeep and maintenance and indicate when they assumed the role.
* A structured approach to mustering documents/assets and when these checks have occurred (a 100% documents/assets muster should be conducted on hand over/take over whenever the incumbents of the responsible officer or supervisor roles are changed).
* If copies of SNI have been formally issued by the dutyholder – both internally and externally – with evidence of a signed receipt.
* All live entries and provide an audit of legacy document control and accounting.

1. Dutyholders are encouraged to adopt a diligent approach to document weeding (purge) to minimise levels of classified holdings through approved destruction procedures and using security approved destruction equipment (refer to TAG 7.4 [18]). A record of the date, responsible person(s) and witness signatures, and the method used for the destruction of above OFFICIAL-SENSITIVE SNI should be reflected in the register.   
   SNI accounted for in the register should be cross-referenced back to the register.

### Inspectors should consider:

* Does the dutyholder have mechanisms and processes in place to categorise SNI, equipment and software in accordance with all relevant classification policy?
* Is there a register which adequately identifies information and associated assets, which denotes value, classification and digital or physical location?
* Does the organisation keep records to control SNI shared and produced by supply chain partners?
* Does the dutyholder account for above OFFICIAL-SENSITIVE:SNI in a dedicated register? If so, does this demonstrate appropriate document control and accounting (such as mustering, disposal and destruction)?

## Identification of Classified Contracts

1. Dutyholders may have contracts with third party[[3]](#footnote-4) suppliers to provide services to systems operating with SNI on the dutyholders’ own sites.   
   The dutyholders risk management process should include any relevant risks from such service provision (e.g., outsourcing of IT system management). Additionally, dutyholders should embed the identification of SNI into a ‘Secure by Design’ process as contracting is often directly integrated into project and programme activity.
2. Dutyholders may also have contracts with third party suppliers for services involving SNI on the third-party sites or IT systems. In such circumstances dutyholders should be aware that they are responsible for the SNI with which they have been entrusted at all times and that this remains the case when they have outsourced a particular service either partially or completely to a third party.
3. Dutyholders should have a mechanism that will identify if SNI is going to be transferred (by any means) or generated as part of the delivery of a specific contract to any third party. The intention is that dutyholders should be able to identify the different levels of risk for specific contracts throughout their supply chain and assure themselves that SNI will be protected.   
   This approach is captured in an ONR principal termed “concentration of risk” that aims to reduce the scope of routine regulatory attention to those areas that present the greatest risk to SNI, consequently reducing the regulatory burden on Industry.
4. This principal is generally used in relation to a specific facility by applying several factors to scope areas subject to routine regulatory attention. Dutyholders should use these factors to establish and document their own guidance for determining which facilities, used by the dutyholder or one of their third parties, should fall inside the scope of ONR’s routine regulatory attention. ONR should be informed of such facilities, likely through being processed through the List N Portal[[4]](#footnote-5). Dutyholders should also maintain a list of facilities, where SNI is handled, which are deemed to fall below the ‘concentration of risk’ threshold, enabling ONR to undertake appropriate sampling and assurance of their process. Appendix 1 expands on the concentration of risk principal.
5. Dutyholders should consider implementing a procedure with a limited set of criteria which can be applied by procurement teams to each contract.   
   This list of questions can operate as part of a risk assessment for each contract providing a value for the level of risk regarding the impact of the compromise of the information and associated assets. The Inherent Risk Profile Questionnaire [19], developed by ONR, is an example method for establishing this risk. Dutyholders utilising the List N Portal will make use of this methodology, but it may be supplemented by other dutyholder approaches.
6. Dutyholder procurement and project teams may require some structured training to confirm that they can correctly identify relevant information and associated assets for each contract. Dutyholders should develop standards, procedures, and arrangements to ensure third parties are made aware of and provided with key information security documentation such as company SNI identification and handling guidance, and incident reporting and handling procedures as part of the contract security aspects letter. They should be made aware of any revisions to this key documentation throughout the contract period. Dutyholders should also consider holding a contract inaugural meeting with third parties to underline and reinforce SNI related assurance expectations and other security related topics such as the reporting and escalation of security incidents/issues, site security policies and practices, and remote working practices etc.
7. In accordance with the requirements from the Cabinet Office Contractual Process [20], dutyholders should have a means of alerting companies bidding for contracts for services or goods that a particular contract will involve SNI assets.
8. Dutyholders should maintain a central register of all third-party contracts involving SNI assets. This register will record which companies are operating with SNI and for what period of time. It may also record details such as the classification of SNI held, details of IT systems processing SNI and potential access to the dutyholders own IT systems or shared cloud environments.
9. The register should be independently reviewed periodically to confirm that it is current. It should function as a trigger for reviews of risk when contracts are added or removed from the list. The register should also capture details of subcontracts that may involve SNI.

### Inspectors should consider:

* Does the dutyholder encourage the early identification of SNI as part of a ‘Secure by Design’ process for projects and programmes?
* Are dutyholders able to clearly identify contracts they have with third parties that involve SNI and associated assets, and how are these managed and maintained?
* Do they have a mechanism for assessing the inherent cyber and information risk for such contracts?
* Is there a mechanism for identifying in third-party contracts the information and associated assets that will be held and/or generated, and their sensitivity?
  + Is this mechanism used down the supply chain and managed effectively?
  + Is the third party provided with key security documentation, including revised copies throughout the contract period?
  + Is a contract inaugural meeting held with the third party to underline and reinforce SNI related assurance expectations?
  + Does the dutyholder maintain a central register of all third party contracts involving SNI assets?

## CS&IA Assessments of Third-Party Suppliers

1. Assessing third party suppliers can be undertaken remotely (using questionnaires), directly by inspection and audit or by a combination of approaches. Dutyholders should consider which approach provides them with adequate assurance, although sample checking should be established where a remote method is relied upon. It should be noted that whilst ONR may conduct direct interventions of third-party suppliers, such activities are undertaken to meet regulatory objectives and are done so on a sampling basis. Dutyholders should not therefore rely upon ONR interventions in lieu of their own assurance and due diligence activities.
2. Dutyholders undertaking their own site survey should consider features from CS&IA methodologies such as: NCSC 10 Steps to Cyber Security [21], the IASME Consortium Cyber Essentials Standard [22], the Center for Internet Security 18 CIS Critical Security Controls [23], NIST Cybersecurity Framework [15], or Annex A of ISO/IEC 27001 [13] amongst others. Consideration should be given to an outcome focussed approach rather than just a checklist of security controls. Such an approach is described in SyAPs FSyP 7 and the associated Annexes F to J and will better prepare third party suppliers for any subsequent ONR intervention activity.
3. ONR has developed the ‘Evidencing Expectations’ question sets [24] which are designed to capture evidence against the principles found in SyAPs:

* FSyP 1 – Leadership and Management for Security
* FSyP 2 – Security Organisational Culture
* FSyP 3 – Competence Management
* FSyP 7 – Cyber Security and Information Assurance
* FSyP 8 – Workforce Trustworthiness.

1. These are aligned to the inherent risk profile levels [19]. Dutyholders utilising the List N Portal will make use of this methodology, but it may be supplemented by other dutyholder approaches.
2. Dutyholders should have a structured approach to the conduct of third-party assessments. The approach must be recordable and repeatable so that results are consistent and should consider the following stages:

* A clearly defined scope for the assessment.
* A process for a review of available evidence to include CS&IA Strategy, CS&IA Policy, Cyber Risk Management approach, Physical Security Plan, Business Continuity and Disaster Recovery plans, Information Asset Register, Risk Register, third party classified contract register, personnel security management, reports from IT Health Checks and technical scans and reports from the incident management process.
* A process for a physical review (internal and external) of security features. Physical and environmental security controls for the protection of SNI should be applied according to layering principles and based on a risk assessment to determine applicable threats and risks in line with guidance set out by the CPNI, as the NTA for Protective Security.
* A mechanism to identify and interview key roles in the organisation to determine if management functions are in place and effective.
* A sampling function could be used to review security controls to confirm that they are effective.
* A reporting function that summarises assessment results in a consistent and traceable manner that can be highlighted to managers and escalated appropriately.
* A process to follow up on identified areas of concern to ensure that they are addressed.

1. When assessing the adequacy of third-party CS&IA measures, dutyholders should assure themselves that the organisation has security measures that meet current good practice and that these measures complement each other in a defence in depth approach. They should also confirm that these measures are implemented by effective procedures and that they are governed by an appropriate management structure. They should consider:

* Has the third party defined ownership of security at a senior level within the business?
* Is cyber and information risk management in place and effective?
* Is the third party physical and personnel security adequate?
* Is third party security for information and associated assets adequate?
* Are both aspects supported by appropriate procedures?
* Does the third party have its own mechanism for gaining independent assurance of its CS&IA arrangements?

1. Advice on the conduct of a site physical security survey is available from CPNI and other organisations. Details of physical security requirements are in TAG 7.4 [18].

### Inspectors should consider:

* Is there an established method for dutyholders to assess third party CS&IA arrangements?
* What third party security measures does the assessment highlight?
* Are the arrangements used by dutyholders to assess CS&IA maturity for third party companies adequate?
* Do the arrangements manage down the supply chain appropriately?
* Are the arrangements consistent with SyAPs?
* Is there any reference to known, reputable methodologies within the assessment?
* Is there a process for ensuring that any issues identified are reported promptly and addressed? Does this encourage a prompt management of any issues? Does it include call out incident reporting?
* Do the arrangements use a structured approach that produces consistent, auditable results that take account of the context of the organisation in scope?
* Does the dutyholder have a mechanism in place for notifying ONR of the initiation and completion of relationships with third party organisations, domestically and internationally, involving the sharing or creation of SNI?

## Assurance of Third-Party Suppliers

1. Inspectors should assure themselves that dutyholders have a mechanism in place to monitor the effectiveness of third party cyber and information risk management throughout the period of their contracts. It is considered good practice that there is at least a review of the assessment on an annual basis and dutyholders should have a process to initiate reviews of third-party CS&IA (this should be part of the contract conditions through a dedicated Security Aspects Letter (SAL) or similar) on an agreed frequency or in response to a notifiable event. The periodicity of review could reflect the level of risk for the contract or the CS&IA maturity of the relevant third-party company as defined by the assessment process.
2. Conditions should be built into the process to ensure that dutyholders are notified in the event of changes that affect the CS&IA risk management posture of the third-party such as:

* A security incident that has or could compromise information and associated assets
* Changes to the business, technology or threats
* Changes of location, company ownership and of security managers

1. In the event that deficiencies are identified in third party contractor risk management, a mechanism is required to address concerns in a timely manner. The requirement for the contractor to do this should be built into the contract and this could include financial penalties for either a failure to address issues completely or for a failure to address them in an agreed timeframe. The dutyholder should also be able to demonstrate notifying the third party of their legal obligations under NISR, as a result of handling SNI and their subjection to ONR regulation as a result.
2. Dutyholders should make every effort to integrate the management of risks to SNI in third party organisations with their own risk management structure. This should include the sharing of threat information, good practice, incident lessons learned or technology changes.
3. A common governance structure could be a useful way of providing visibility of concerns and of sharing possible solutions to problems. One such structure is the Security Working Group which can run both internally within an organisation, but which could usefully include third party suppliers as well as external expertise from regulators and others.

### Inspectors should consider:

* Does the dutyholder have a mechanism to assess and review CS&IA arrangements for third party companies on a continuing basis?
* Are third party suppliers obliged to inform the contracting organisation of any changes which might impact their security posture – including arrangements to control and assure activities involving sub-contracts?
* What is the reporting process and governance structure if such issues are identified?
* Are the results of the assessments fed back by adequate reporting and are they reflected in dutyholder central risk management functions such as the risk register?
* Is there an adequate governance structure?
* Are the above expectations defined in contractual arrangements i.e. through a Security Aspects Letter (SAL) or similar?

## End of Contract

1. There should be a clear understanding between dutyholders and third-party contractors of what will happen to information and associated assets at the end of the contract period, or the end of the period during which the contractor is required to hold the information and associated assets (whichever is longer). The dutyholder should ensure that the requirements around this are made clear at the outset of the engagement and are embedded in the contract. This is because in many instances the requirements will need to be included in the technical solution and will have cost implications for delivering the contract to both parties.
2. The approach to data management at the end of a contract will vary dependent upon if there is a likelihood of a re-engagement on similar work within a reasonable time frame. In such an event dutyholders could take a risk-based approach.
3. If information and associated assets are retained by the third party for any time beyond the formal contract, dutyholders should assure themselves that it remains appropriately protected. However, dutyholders may also consider having all information and associated assets returned to them regardless and store it themselves until a fresh contract is in place.
4. Assuming that there is no follow-on contract requirement, dutyholders should have a process for all information and associated assets to be either returned or destroyed securely. Dutyholders should have a registry of exactly what type and sensitivity of information and associated assets are held, in what format, and by which third party contractors. The register should be used to issue instructions on which assets are to be returned and which destroyed securely, and how. Further guidance on the appropriate methods of destroying classified information can be found in TAG 7.4 [18].
5. Dutyholders should ensure that they have an asset management process that identifies when information and associated assets have been returned or destroyed appropriately in line with current NTA RGP as provided in   
   TAG 7.4 [18]. This process should be supported by evidence such as destruction certificates and data transfer documentation. For legal, contractual and financial reasons, information relevant to the contract may need to be retained for a number of years. It is unlikely but still possible that SNI may be contained in that material. Dutyholders should consider a risk managed approach on how it is to be protected and should assure themselves that third parties are aware of the need to protect it adequately for as long as it is held. In these cases, dutyholders should continue their management of the contractor CS&IA risk as before, but potentially with redefined assurance timescales and review milestones.
6. It should be noted in instances where third party suppliers have a legitimate need to retain SNI, they remain subject to regulatory interventions by ONR.

### Inspectors should consider:

* Does the dutyholder have a process to manage the closure of contracts with third party companies involving information and associated assets?
  + Is it enforceable through conditions within the contract(s)?
  + Does the dutyholder have a mechanism for handling situations where the third party is required to handle SNI beyond the closure of the contract?
* Is there an established process for returning or securely destroying information and associated assets from third parties, if so, what is it?
* Are there adequate arrangements captured in relevant standards, procedures and arrangements, in line with current NTA RGP, for the secure disposal of SNI as part of the end of contract process.
* Is there a process that requires evidence of asset transfer and destruction and is this reflected in the dutyholder asset and risk management registers?
* If information and associated assets stay with the third party post formal contract period, what is the assurance for appropriate and adequate protection?

# References

|  |  |
| --- | --- |
| [1] | ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” 2017. |
| [2] | HM Government, “The Nuclear Industries Security Regulations 2003 (NISR),” 2003. |
| [3] | HM Government, “Government Functional Standard GovS 007: Security,” 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/1016424/GovS\_007-\_Security.pdf. |
| [4] | HM Government, “Security Policy Framework,” February 2022. [Online]. Available: https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework. |
| [5] | HM Government, “Government Security Classification (Version 1.1),” 2018. |
| [6] | ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry,” November 2021. [Online]. Available: https://www.onr.org.uk/documents/classification-policy.pdf. |
| [7] | IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”. |
| [8] | IAEA, “Nuclear Security Series (NSS),” [Online]. Available: https://www.iaea.org/resources/nuclear-security-series. |
| [9] | IAEA, “Nuclear Security Series No. 20 - Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime,” 2013. |
| [10] | IAEA, “Nuclear Security Series No. 13 - Nuclear Security Recommendations on the Physical Protection of NUclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011. |
| [11] | IAEA, “Nuclear Security Series No. 23-G IAEA Implementing Guide: Security of Nuclear Information,” 2015. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf. |
| [12] | IAEA, “Nuclear Security Series No. 17 - Computer Security techniques for Nuclear Facilities”. |
| [13] | ISO, “ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements,” 2013. |
| [14] | International Society of Automation/International Electrotechnical Commission (ISA/IEC), “ISA/IEC 62443 Series of Standards,” [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. |
| [15] | NIST, “Cybersecurity Framework,” [Online]. Available: https://www.nist.gov/cyberframework. |
| [16] | ONR, “CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management”. |
| [17] | ONR, “CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations”. |
| [18] | ONR, “CNS-TAST-GD-7.4 - Physical Protection of Information”. |
| [19] | ONR, “Nuclear Industry Security Regulations - Regulation 22 Dutyholder: Inherent Risk Profile Question Set,” April 2023. [Online]. Available: https://www.onr.org.uk/cnss/regulation-of-sensitive-nuclear-information-list-n.htm. |
| [20] | Cabinet Office, “Contractual Process (Version 7.3),” May 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/710891/2018\_May\_Contractual\_process.pdf. |
| [21] | NCSC, “Guidance: 10 Steps to Cyber Security,” [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps. |
| [22] | IASME Consortium, “Cyber Essentials,” [Online]. Available: https://iasme.co.uk/cyber-essentials. |
| [23] | Center for Internet Security (CIS), “The 18 CIS Critical Security Controls,” [Online]. Available: https://www.cisecurity.org/controls/cis-controls-list. |
| [24] | ONR, “Regulation of Sensitive Nuclear Information (SNI) in the Supply Chain (List N),” [Online]. Available: https://www.onr.org.uk/cnss/regulation-of-sensitive-nuclear-information-list-n.htm. |

# Glossary and Abbreviations

CA Contracting Authority

CPNI Centre for the Protection of National Infrastructure

CPPNM Convention on the Physical Protection of Nuclear Material

CS&IA Cyber Security and Information Assurance

FSyP Fundamental Security Principle

GovS 007 HMG Government Functional Standard 007, Security

GSC HMG Government Security Classifications

HMG His Majesty’s Government

IAEA International Atomic Energy Agency

IAR Information Asset Register

IAEA International Atomic Energy Agency

IEC International Electrotechnical Commission

ISA International Society of Automation

ISF Information Security Forum

ISO International Organisation for Standardisation

IT Information Technology

NCSC National Cyber Security Centre

NISR Nuclear Industries Security Regulations 2003

NIST National Institute of Standards and Technology

NM Nuclear Material

NSS Nuclear Security Series

NTA National Technical Authority

ONR Office for Nuclear Regulation

ORM Other Radioactive Materia

OT Operational Technology

RGP Relevant Good Practice

SNI Sensitive Nuclear Information

SO Official Committee on Security

SPF Security Policy Framework

SyAP Security Assessment Principle

SyDP Security Delivery Principle

TAG Technical Assessment Guide

US NRC United States Nuclear Regulatory Commission

# Appendix 1 – Concentration of Risk

1. ONR has broad powers under Regulation 22 of NISR 2003 that, if exercised in full, could be considered to be disproportionate in some instances when measured against the associated risk.
2. As such, ONR chooses to focus regulatory resource and attention on areas where there is deemed to be a greater concentration of inherent risk to SNI, consequently reducing the regulatory burden on Industry. This principal is generally used to consider the focus of routine regulatory attention in relation to a specific facility handling, storing or processing SNI.
3. It should be noted that this does not restrict ONR’s powers or ability to enforce in areas outside of this, should an incident or security failing be identified.
4. This principal uses the following factors to scope areas subject to routine regulatory attention, in relation to the protection of SNI:

* Classification
* Frequency of access
* Duration
* Format of SNI being accessed and whether it is stored at the facility
* The organisation controlling the security of the SNI
* Location and environmental factors
* Quantity of SNI

1. Dutyholders should use these factors to establish and document their own guidance for determining which facilities, used by the dutyholder or one of their third parties, should fall inside the scope of ONR’s routine regulatory attention. ONR should be informed of such facilities, likely through being processed through the List N Portal. Dutyholders should also maintain a list of facilities, where SNI is handled, which are deemed to fall below the ‘concentration of risk’ threshold, enabling ONR to undertake appropriate sampling and assurance of their process.
2. As an example, it would generally not be appropriate for employees of a dutyholder working on O-S:SNI from home to have their home addresses recorded as facilities on the List N Portal. This would be because of the likely lower frequency, duration and quantity of SNI being worked upon.   
   They would also fall under the dutyholders standards, procedures and arrangements which should include guidance, training and assurance activity along with close working relationships with their manager to ensure that they maintain appropriate behaviours and comply with the organisations security policies. Such logic may also apply to an Agency Support Worker, where they are assigned a manager within the CA organisation and managed in a similar way to members of staff.
3. However, should a similar assessment be undertaken on a member of staff of a third-party organisation working on SNI at home, it may be deemed that a corporate List N approval would be required to assess whether the   
   third-party organisation has appropriate home working policies, along with a mature security culture and adequate risk management processes etc. Whilst the contractor employee’s home address may still not be subject to a List N assessment and approval, the organisation should have obtained a List N approval to demonstrate that they have suitable standards, procedures and arrangements to effectively manage the risks to SNI under their care.
4. Applying a similar situation to a small third-party company whose home is also their base of business operations, it may in some circumstances be appropriate for their home to be subject to a List N assessment and approval. This is because they are not part of a larger organisation and their standards, procedures and arrangements relating to the protection of SNI may relate solely to that location.
5. Whilst such parameters may deem a location or facility to fall outside of routine regulatory attention, the dutyholder should still consider risks to SNI at such locations and implement suitable standards, procedures and arrangements to ensure its protection. For the example of a dutyholders employee working on SNI from home, this could include:

* Home working policies
* An approvals process for working on SNI from home
* Guidance to individuals working from home
* A checklist for considering the suitability of an individual’s home working environment for working on SNI
* Internal assurance processes
* Provision of suitable equipment to mitigate risks such as privacy screens and lockable cabinets.

1. This list is not considered to be exhaustive or mandatory but should give an indication of the types of controls an inspector may look for when assessing the associated standards, procedures, and arrangements. In all instances inspectors should provide advice and guidance to contracting authorities where requested.

1. The security classification levels for SNI are OFFICIAL-SENSITIVE, SECRET and potentially TOP SECRET. [↑](#footnote-ref-2)
2. Consult CWP/G5 and CCSWG if information relates to the enrichment of uranium. [↑](#footnote-ref-3)
3. Third party suppliers handling, processing and storing SNI are Regulation 22 dutyholders under NISR. For clarity these external bodies are referred to in the classified contract components of this TAG as a ‘third party’, whilst ‘dutyholders’ refers to those contracting authorities (CA) that manage classified contracts. [↑](#footnote-ref-4)
4. An online regulatory portal enabling contracting authorities (CA) to undertake Facility Security Clearances (FSCs) of dutyholders subject to Regulation 22 of NISR 2003, informally known as List N dutyholders. [↑](#footnote-ref-5)