ONR GUIDE			
CYBER SECURITY AND INFORMATION ASSURANCE			
Document Type:	Nuclear Security Technical Inspection Guide		
Unique Document ID and Revision No:	CNS-INSP-GD-7.0 Revision 0		
Date Issued:	January 2018	**Review Date:**	January 2021
Approved by:	Matt Sims	Professional Lead Security Specialism	
Record Reference:	TRIM Folder 4.4.2.20789. (2017/456631)		
Revision commentary:	New Document Issued		

TABLE OF CONTENTS

1 INTRODUCTION

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

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

1.3 The Office for Nuclear Regulation (ONR) has established a set of outcome focused Security Assessment Principles (SyAPs) (Reference 6.1) which provide a framework for it to assess security arrangements defined in security plans and make consistent regulatory judgements on the adequacy of those arrangements. The Fundamental Security Principles (FSyPs) and their underpinning Security Delivery Principles (SyDPs) are goal-setting and do not describe what the dutyholder's arrangements should contain; this is the responsibility of the dutyholders who remain responsible for security.

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

2 PURPOSE AND SCOPE

2.1 Security plans should be structured in a format consisting of high-level claims, supported by arguments substantiated by evidence. Where the dutyholder is required to have an approved security plan, the purpose of this guide is to facilitate a consistent and effective approach to inspecting compliance with the arrangements detailed in the plan concerning FSyP 7 - Cyber Security and Information Assurance (CS&IA). This fundamental principle is supported by five Technical Assessment Guides (TAGs): Effective Cyber and Information Risk Management (Reference 6.2); Information Security (Reference 6.3); Protection of Nuclear Technology and Operations (Reference 6.4); Physical Protection of Information (Reference 6.5); and Preparation for and Response to Cyber Security Incidents (Reference 6.6).

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

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

associated arguments. The inspector may also provide advice and guidance in the interests of encouraging dutyholders to seek continuous improvement.

2.3 Where SNI is held at locations other than nuclear premises or by an approved carrier, Regulation 22 places a requirement to implement standards and arrangements to minimise the risk of loss. These dutyholders are not required to detail these arrangements in an approved plan. Therefore, ONR forms judgments of adequacy of compliance against Regulation 22 requirements against the SyDPs and TAGs relating to FSyPs 1, 2, 3, 7 & 8 because they incorporate government expectations for CS&IA as articulated in the HMG Security Policy Framework. Further information on conducting inspections of these locations is provided at section 5.

2.4 This guidance is not intended to be mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections.

2.5 This guidance does not indicate when or to what extent these compliance inspections should be made. These matters are covered in the integrated intervention strategy and individual inspectors' inspection plans.

2.6 This guide lays the foundation for all inspection activities carried out by CS&IA inspectors. The same basic phases should be applicable to an inspector in any of the ONR Divisions. The phases which will help inspectors plan their inspection programmes and CS&IA compliance inspections are: planning, preparation, delivery, write up, and follow up. For more detailed information on these phases see ONR Guide GD-064 (Reference 6.7).

2.7 Relevant good practice that can be used to support FSyP 7 inspection activity is available at an international and national level. These include International Atomic Energy Agency (IAEA) Nuclear Security Series documents NSS 13, 17, 20 and 23G. In particular, Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, 'Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)'(Reference 9.2) incorporates issues pertaining to confidentiality within Fundamental Principle L.

3 OVERVIEW OF FUNDAMENTAL SECURITY PRINCIPLE 7: CYBER SECURITY AND INFORMATION ASSURANCE

3.1 FSyP 7 details that dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.

3.2 SyDP 7.1 describes that dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively.

3.3 SyDP 7.2 outlines the information security expectations that dutyholders should maintain the confidentiality, integrity and availability of SNI and associated assets.

3.4 SyDP 7.3 concerns the protection of nuclear technology and operations. It details that dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.

3.5 SyDP 7.4 describes the expectations for the physical protection of information. Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.

3.6 SyDP 7.5 concerns arrangements for the preparation for and response to cyber security incidents. It details that dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.

4 GUIDANCE ON THE EXPECTATIONS FOR THE INSPECTION OF FSYP 7

4.1 **Planning Phase -** ONR CNS has developed regulatory strategies for dutyholders. This includes conducting a programme of CS&IA interventions to influence CS&IA behavioural changes across the industry. For all of the major sites and facilities, an annual CS&IA Integrated Intervention Strategy (IIS) plan exists which describes how the strategy is realised through a series of planned inspections. For more detail on IIS plans, see ONR Guide GD-059 (Reference 6.10).

4.2 In addition to following guidance on the planning phase contained in ONR Guide GD-064 (Reference 6.7), when preparing CS&IA interventions inspectors should:

- Review the CS&IA IIS plan to confirm the inspection is on the plan, or if necessary, that the plan is modified to include the planned inspection.
- Consult with the nominated site security inspector (where applicable) to ensure they are fully aware of all inspection activities taking place and can support and give a regulatory context.
- Identify which ONR inspectors (safety and security), technical advisers and internal regulators will be involved.

4.3 **Preparation Phase -** In addition to following guidance on the preparation phase contained in ONR Guide GD-064 (Reference 6.7), when preparing CS&IA interventions inspectors should:

- Review the inspection history for the site/dutyholder. Previous IRs and the RID should be reviewed to determine if there are legacy concerns or issues outstanding which are relevant to the planned inspection.
- Consult the site security inspector (where applicable) to understand the current regulatory context, and any relevant compliance documentation. This context could include: current and recent issues; enforcement activity; inspection history; regulatory topics and themes that the planned inspection should align with.
- Thoroughly review the approved security plan, selecting arguments and evidence that will be sampled to form the basis of the inspection.
- Review relevant guidance, in conjunction with relevant good practice, to develop a clear understanding of the standards that are expected. Inspectors should consider whether dutyholders have designed and implemented a proportionate Cyber Protection System that achieves the relevant security outcome and posture using the graded approach. The scope of the inspection should be decided and articulated through the preparation of an appropriate question set. Consider using ‘the Inspectors should consider’ questions from the appropriate TAG.

4.4 **Implementation - General** - Information on implementing the delivery, write up and follow up phases is contained in ONR Guide GD-064 (Reference 6.7).

Taking into Account Other FSyPs

4.5 Inspectors should take into account other FSyPs when carrying out CS&IA inspections, in particular: FSyP 3 (Competence Management); FSyP 4 (Nuclear Supply Chain Management); and FSyP 5 (Reliability, Resilience and Sustainability). For example:

- Are the dutyholder's CS&IA staff suitably qualified and experienced to carry out their assigned security roles and responsibilities?
- Do dutyholders implement and maintain effective supply chain management arrangements for the procurement of products or services related to CS&IA?
- Have dutyholders designed and supported their CS&IA regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle?

Specific Advice for CS&IA Inspections

4.6 Specific considerations related to the arrangements for each of the FSyP elements are covered in the Annexes as follows:

- Annex A - SyDP 7.1 (Effective Cyber and Information Risk Management).
- Annex B – SyDP 7.2 (Information Security).
- Annex C – SyDP 7.3 (Protection of Nuclear Technology and Operations).
- Annex D – SyDP 7.4 (Physical Protection of Information and Information Assets).
- Annex E – SyDP 7.5 (Preparation for and Response to Cyber Security Incidents).

5 GUIDANCE ON THE EXPECTATIONS FOR THE INSPECTION OF LOCATIONS HOLDING SNI

5.1 SNI is defined under the Anti-terrorism, Crime and Security Act 2001 as information relating to, or capable of use in connection with, the enrichment of uranium; or information relating to activities carried out on or in relation to nuclear sites or other nuclear premises which appears to the Secretary of State to be information which needs to be protected in the interests of national security.

5.2 The Nuclear Industries Security Regulations (NISR) 2003 further amplifies this definition to include:

- Information which requires a classification in accordance with the classification policy, thus defined as "information concerning the use, storage and transport of nuclear and other radioactive material"[2], issued by the Secretary of State.

[2] NISR Classification Policy (TRIM 2017/368348).

- Information which bears a classification which has been applied by a Government Department or a statutory body in the interests of national security.

5.3 Furthermore the Energy Act 2013 added a further definition of SNI to include:

- Information relating to, or capable of use in connection with, the enrichment of uranium.
- Information of a description for the time being specified in a notice under Section 71. This applies where the Secretary of State considers that information of any description relating to activities carried out on or in relation to civil nuclear premises is information which needs to be protected in the interests of national security.

5.4 As detailed in paragraph 2.3 above, SNI may be held in locations for which there is no approved security plan or transport security statement. However, the responsible persons for this information are still legally required to protect it in accordance with Regulation 22 and ONR are still expected to undertake activity (which may be on a sampling basis) that provides assurance that adequate CS&IA arrangements are being maintained. Where this activity includes inspections (both announced and unannounced), the planning and preparation phases are equally as important and relevant as they are for nuclear premises or approved carriers.

5.5 The specific wording of Regulation 22 states that a person to whom the regulation applies must:

> *'maintain such security standards, procedures and arrangements 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 his possession or control'*

5.6 Applied literally, the implication of the use of the term 'minimise' is that dutyholders must continue to apply risk mitigation controls until there are no other measures that can be applied, regardless of considerations of SNI security classification, time, money or effort. To adopt this approach would be contrary to the principles of the Regulators Code[3] and inconsistent with how ONR regulates wider aspects of security, using the graded approach; or safety, through demonstration that risks have been reduced to As Low As Reasonably Practicable.

5.7 In order for regulation to be effective, it must be equally clear to dutyholders how they demonstrate that they have achieved compliance and for regulators to demonstrate where they have not in order to allow them to be held to account. The HMG Security Policy Framework (SPF) published by the Cabinet Office describes the Cabinet Secretary and Official Committee on Security's 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. Accordingly, ONR consider this publication to set out appropriate relevant good practice for the protection of SNI. The SPF contains eight security outcomes supported by twenty-nine requirements. These outcomes and requirements have been adapted to reflect ONR's Regulation 22 vires and incorporated into the ONRs SyAPs under the following FSyPs:

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300126/14-705-regulators-code.pdf

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

5.8 The purpose of this integration is to provide a single source of relevant good practice that can be used for assessment and/or inspection of CS&IA across the range of NISR dutyholders whether they are public or private entities, ensuring consistency of approach and regulatory expectation. Therefore, these FSyPs, together with the associated Security Delivery Principles and TIGs should be used as the inspection framework against which judgements are made as to the adequacy of CS&IA arrangements of locations subject to Regulation 22. The table at Annex F shows the linkage between SyAPs and the HMG SPF.

5.9 In addition to the FSyPs detailed above, inspectors should note that FSyP 4 sets a regulatory expectation that contracting authorities will implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security. FSyP 4 is supported by four SyDPs; SyDP 4.2 relates to supplier capability and states that for work that may impact on nuclear security, dutyholders should evaluate and confirm that suppliers have the organisational and technical capability, capacity and culture to deliver items or services to the specification prior to placing any contract. SyDP 4.3 relates to oversight of suppliers of items or services that may impact on nuclear security and states that dutyholders should conduct effective oversight and assurance of their supply chain. Therefore, inspectors should consider using inspections of Regulation 22 dutyholders to provide assurance that contracting authorities are achieving regulatory expectations with respect to their supply chain management arrangements. Questions may include:

- How did your contracting authority engage with you to during the tender process to ensure you had the technical capability and capacity to deliver the contract to specification?
- How has your contracting authority maintained oversight and assurance of the contract?

5.10 The Regulation 22 community is highly diverse and spans facilities that employ one or two members of staff with minimal holdings of SNI, to those that employ many hundreds and have significant inventories of high security classification SNI. It is therefore essential that inspectors apply proportionality when conducting a regulation 22 compliance inspection. For example, FSyP 3 articulates a formal and systematic approach to training. Whilst this would be appropriate for a large organisation, it would be hard to justify for a two-person business. Instead, in the case of the latter it would be reasonable to expect that the individuals were adequately qualified and experienced to protect SNI effectively and the company policy incorporates a commitment to maintain the skills necessary to sustain compliance. In either example evidence should be sought to demonstrate appropriate arrangements are in place.

5.11 In light of this diversity, inspectors should note that there are no model standards or prescription at the operational level, nor is it appropriate for there to be in an outcome

focused regulatory regime. Instead, it is up to dutyholders to fully justify their own arrangements; and for inspectors to use their knowledge and experience when forming judgements regarding Regulation 22 compliance.

5.12 Unlike Regulation 4 (nuclear premises) or Regulation 16 (approved carriers) dutyholders, NISR places no requirement on Regulation 22 dutyholders to detail their CS&IA arrangements within a security plan approved by ONR. However, Regulation 22 dutyholders are strongly recommended to produce such documentation (referred to from now on as a CS&IA plan), which they can use to inform their business operations and provide self-assurance that they are meeting their obligations to protect SNI under NISR.

5.13 The principle of proportionality also applies in the production of CS&IA plans. This means that for a dutyholder with substantial holdings of highly security classified SNI and/or where digital SNI is held on systems connected to the internet, a robust CS&IA plan constructed of claims, supported by arguments and justified by a complete evidence suite is likely to be appropriate. Conversely, where a dutyholder's inventory of SNI is no higher than OFFICIAL-SENSITIVE, and digital information is limited to stand-alone or Local Area Networks (with no Internet connection), then a simpler approach may be appropriate. For those dutyholders that meet the latter description of SNI holdings, ONR have produced a template at Annex G, which may be used as the basis for production of a proportional CS&IA plan, again recognising that this will still need to be tailored to the facility in question.

5.14 Where dutyholders have produced a CS&IA plan and made it available to ONR, inspectors should complete an office-based assessment prior to any inspection. Where information is complete and the arrangements are judged to be adequate at this stage, inspectors may determine that a site inspection is not necessary. However, an inspection may still be considered appropriate, particularly where a dutyholder has larger quantities of SNI. In these instances, inspectors may select a sample of evidence and limit both the duration and scope of any inspection to that required for onsite verification of the sample. Conversely, where there is no CS&IA plan or suitable comparative document suite available, ONR inspectors should undertake inspections to collect evidence of Regulation 22 compliance. These inspections are likely to be more frequent and of greater duration than would otherwise be the case where a CS&IA plan is available. Therefore, whilst not a regulatory requirement, the production of a CS&IA plan that is submitted to ONR for review is likely to result in reduced regulatory burden provided the submission is of adequate quality, accurate and the arrangements it describes are effectively implemented.

5.15 Contracting authorities may also take a similar approach to that described above when seeking assurance of their supply chain. This could be reinforced by making the production, maintenance and implementation of a CS&IA plan a contractual obligation. Furthermore the existence of a CS&IA plan may provide additional benefits for contractors when dealing with multiple contracting authorities who are likely to require similar levels of assurance.

6 FURTHER READING

6.1 Security Assessment Principles for the Civil Nuclear Industry.

6.2 CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management.

6.3 CNS-TAST-GD-7.2 - Information Security.

6.4 CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations.

6.5 CNS-TAST-GD-7.4 - Physical Protection of Information.

6.6 CNS-TAST-GD-7.5 - Preparation for and Response to Cyber Security Incidents.

6.7 CNS-INSP-GD-001 – Leadership and Management for Security

6.8 CNS-INSP-GD-002 – Organisational Culture

6.9 CNS-INSP-GD-008 – Workforce Trustworthiness

6.10 NISR 2003 Classification Policy for the Civil Nuclear Industry

6.11 ONR GUIDE GD-064 - General Inspection Guide.

6.12 IAEA Safety Standard No GS-R-3 (The Management System for Facilities and Activities).

6.13 IAEA Nuclear Security Fundamentals NSS 20 - Objective And Essential Elements of a State's Nuclear Security Regime.

6.14 ONR Guide GD-059 - Guidance for Intervention Planning and Reporting.

7 ANNEX A - EFFECTIVE CYBER AND INFORMATION RISK MANAGEMENT

Regulatory Expectation

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

Inspectors should consider the dutyholder's ability to demonstrate compliance with their security plans through the exhibition of behaviours and knowledge, and the provision of evidence. This may include:

Scope and Business Objectives

- Check that there is a clear understanding of how the organisation is structured and how it interacts with partners and suppliers.
- Confirm that there is a clear view of where digital and information assets are within the business.
- Establish that the business objectives for cyber and information risk management have been defined.
- Check that there are risk appetite statements for critical business functions and that they are appropriate.
- Verify whether relevant legislation and regulation have been identified.

CS&IA Risk Governance Structure

- Check whether it is clear throughout the organisation who has responsibilities for risk management.
- Verify that key roles (such as the Senior Information Risk Owner) have been filled and that the details are current.
- Seek evidence that post holders are suitably qualified and experienced for their roles.
- Check that there is a CS&IA Policy and it is appropriate to the organisation:
  - Is it current and has it been endorsed by the Board?
  - Is it resourced adequately?
  - Is it easily available to all personnel (to include partners and suppliers as necessary)?
  - Is there a mechanism for communicating updates?
  - Is there a monitoring, review and reporting process to identify either areas of weakness or non-compliance?

CS&IA Risk Management Approach

- Establish whether there is a defined approach for how risk management will be carried out in the organisation:
  - Does it include partners and suppliers?
- Determine whether risk management is considered in the planning for new systems.
- Confirm whether their risk management approach covers the whole lifecycle for the information assets:
  - Does it cater for regular risk reviews?
  - Does it include change control?

  - Does system planning include notifying ONR of any new IT operational system or high risk system within a suitable time frame?
- Check whether there is a risk management communications plan and it is appropriate.

CS&IA Risk Assessment Approach

- Taking a proportionate approach, establish that the risk assessment methodology is appropriate for the size and scope of the organisation:
  - Is it operated by suitably qualified and experienced personnel?
  - Is it auditable?
- Check whether the risk assessment considers risks from partners and supply chain companies.
- Confirm by sampling that the threat assessment is informed from relevant sources and it covers the correct scope.

CS&IA Risk Treatment Approach

- Sample security controls to confirm that they have been selected to mitigate risks identified from a risk assessment.
- Check that there is evidence of a clear mapping of security controls to identified risks.
- Look for evidence of assurance functions tailored to the level of risk and the risk appetite of the business.
- Check that there is evidence that the assurance process is planned and resourced for the lifetime of the information assets.
- Discuss with risk managers how they assess effectiveness.

CS&IA Residual Risk Management

- Discuss with managers how risks are presented and explained to them.
- Seek evidence that risk managers at all levels understand their role in the governance structure, they are empowered appropriately and there are clear escalation paths.
- Check that there is a defined structure for capturing and presenting residual risk to managers.
- Confirm that it is clear who owns residual risk for each system.
- Check whether there is a mechanism for identifying CS&IA risks from different operational areas and reporting significant risks to senior managers and ultimately to the Board.
- Ensure that the risk management process operates over the lifetime of information assets.

The following documents are representative of evidence that may be referenced in the security plan and should be sought for review prior to the inspection:

- Business objectives.
- Security post holders and their qualifications and experience.
- CS&IA Policy.
- Risk appetite statements.
- Risk management communications plan.
- Risk assessments.

- Threat assessments.
- Risk registers.
- Cyber Protection Systems.

8 ANNEX B - INFORMATION SECURITY

Regulatory Expectation

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.

Inspectors should consider the dutyholder's ability to demonstrate compliance with their security plans through the exhibition of behaviours and knowledge, and the provision of evidence. This may include:

CS&IA Policy and Standards

- Confirm that the dutyholder has a CS&IA strategy that is appropriate to the organisation.
  - Is the strategy adequate to identify and manage risks to information and associated assets?
- Check that the dutyholder has a CS&IA policy in place that is scoped to the organisation.
  - Are all relevant topics adequately addressed?
  - Does the policy reflect relevant good practice?

Data Classification and Sensitivities

- Check that the dutyholder has mechanisms and processes in place to categorise SNI, equipment and software within all relevant classification policies.
- Check that there is a register which adequately identifies SNI and relevant equipment and software, if so, examine samples from the register to ensure that they denote value, classification and digital or physical locations.

Identification of Classified Contracts

- Confirm that dutyholders are able to clearly identify contracts they have with third-parties that involve SNI and associated assets.
- Establish that they have a mechanism for assessing the cyber and information risk for such contracts.
- Check there is a mechanism for identifying in third-party contracts the information and associated assets that will be held and/or generated, their sensitivity and how they are to be protected.
  - Is this mechanism used down the supply chain and managed effectively?

CS&IA Assessments of Third-Parties

- Check the arrangements used by dutyholders to assess CS&IA maturity for third-party companies to confirm that it is adequate.
- Confirm that the scope of the arrangements is adequate.
- Confirm that the arrangements manage down the supply chain appropriately.
- Establish whether the dutyholder has confirmed the contractor's arrangements are consistent with SyAPs.
- How do they ensure that any issues identified are reported promptly and addressed?

- Check that the arrangements use a structured approach that produces consistent, auditable results that take account of the context of the organisation in scope.

Assurance of Third-Parties

- Establish how the dutyholder assesses and reviews CS&IA arrangements for third-party companies on a continuing basis.
- Check that it is supported by contractual conditions that provide for a response in the event of deficiencies arising.
- Discuss with the relevant person how the results of the assessments are fed back by adequate reporting and are reflected in dutyholder central risk management functions such as the risk register.
- Check that there is an adequate governance structure.

End of Contract

- 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)?
- Check that the dutyholder gives clear guidance on which assets are to be returned or destroyed securely.
- Establish whether there is a process that requires evidence of asset transfer and destruction and is this reflected in the dutyholder asset and risk management registers.

The following documents are representative of evidence that may be referenced in the security plan and should be sought for review prior to the inspection:

- CS&IA Policy.
- Register of Classified Contracts.
- CS&IA Strategy.
- Classified Contracts Policy.

9 ANNEX C - PROTECTION OF NUCLEAR TECHNOLOGY AND OPERATIONS

Regulatory Expectation

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

Inspectors should consider the dutyholder's ability to demonstrate compliance with their security plans through the exhibition of behaviours and knowledge, and the provision of evidence. This may include:

System Dependencies

- Confirm that there is a clear understanding of what technology is in scope.
- Check that there is an effective categorisation methodology in place that is appropriate to the organisation:
  - Is it aligned with the framework provided in SyAPs Annexes F and G?
  - Is it auditable and does it provide consistent results?
  - Does it cover partners, service providers and suppliers?
- Establish that system dependencies have been identified adequately.

Achieving the Cyber Protection System Outcome and Response Strategy

- Confirm that the dutyholder has selected the correct Cyber Protection System (CPS) outcome(s) for the technology concerned.
- Check by sampling that claims and arguments made in respect of achieving the CPS outcomes are supported by sound evidence (e.g. through conduct of a structured and systematic approach to advanced threat penetration testing such as that developed and deployed recently in the financial sector; classified material assessment tool findings; or expert judgement from organisations such as the National Cyber Security Centre (NCSC)).
- Ensure that there has been appropriate interface between the dutyholder and all organisations providing elements of the CPS.

Security Control Principles

- Ask the dutyholder to demonstrate how the selection of technical cyber security controls is based upon a risk assessment and is aligned with the SyAPs.
- Check that the controls are used within a defence in depth approach.
- Confirm that the dutyholder has an adequate mechanism for testing control implementations.
- Seek evidence that control implementations are actively managed by a monitoring process that reflects changes in risk.
- Evaluate how the dutyholder ensures that their control assessment and implementation process can scale up as required.

Resilience and Assurance of Controls

- Verify that the categorisation methodology has been used to help define the level of assurance required.
- Seek assurance that if component assurance was required, the use of evaluated products was considered.

- Check that if technical testing was planned, it was conducted by SQEP personnel.
- Confirm that assurance (all types) is planned for the lifetime of the information asset.
- Check by sampling that each IT/OT system is supported by independently verified documentation that identifies the risks to that system and confirms that those risks have been mitigated to an acceptable level.

The following documents are representative of evidence that may be referenced in the security plan and should be sought for review prior to the inspection:

- System policies.
- Security Operating Procedures.
- Risk Management Accreditation Document Sets.
- System Operating Procedures.
- IT Health Checks.
- Vulnerability assessments.
- Penetration tests.
- Network diagrams.
- Firewall rule sets.

10 ANNEX D - PHYSICAL PROTECTION OF INFORMATION

Regulatory Expectation

The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements for the physical protection of information and associated assets in support of maintaining effective CS&IA arrangements.

Inspectors should consider the dutyholder's ability to demonstrate compliance with their security plans through the exhibition of behaviours and knowledge, and the provision of evidence. This may include:

Physical Security Risk Assessment

- Confirm that the physical security measures are part of a layered approach based upon a risk assessment.
- Check that the risk assessment adequately considers all relevant threats.
- Ensure that an appropriate specification (such as an Operational Requirement) has been produced and used to design the physical protection of information and associated assets.

Physical Security Control Measures

- Check that a physical security plan or similar has been developed to describe the controls in place and it is appropriate.
- Assure by sampling that physical security measures for buildings, rooms and containers are appropriate for the level of risk.
- Where AACS systems are in place, check that measures for their protection have been implemented.
- Confirm that area alarms are of an adequate standard and they are monitored appropriately.
- Seek evidence that the alarm response force is trained and resourced adequately to respond to physical security events that affect SNI.
- Check that the purpose of CCTV systems has been clearly defined and the technical implementation is adequate.
- Confirm that consideration was given to the siting of technology.
- Evaluate how cable layout and security are part of a planned and structured process.
- Discuss with the appropriate person whether TEMPEST considerations for the site have been assessed and mitigated adequately where appropriate.
- Seek evidence that secure disposal mechanisms are being implemented.
- Check that risks to the operation of environmental management systems been identified and mitigated adequately.

Assurance of Physical Security Measures

- Confirm that there is adequate assurance that physical security measures are effective:
  - Is there a process for monitoring and for identifying and addressing deficiencies?
- Check that there is confidence that changes to threats, technology or the business are reflected in a review of security measures as part of the change management process:

  - Is there assurance that physical security measures can be scaled up as necessary?
- Confirm by sampling documentation that all physical security measures are adequately supported by procedural and personnel measures.
- Establish how the dutyholder ensures that risks to SNI held within its supply chain are appropriately managed.

The following documents are representative of evidence that may be referenced in the security plan and should be sought for review prior to the inspection:

- Physical Protection of Information policy.
- Physical Protection of Information procedures.
- Risk assessments.
- Physical protection systems.
- Operational requirements.
- Completed Classified Material Assessment Tools.
- Details of security controls.

11 ANNEX E - PREPARATION FOR AND RESPONSE TO CYBER SECURITY INCIDENTS

Regulatory Expectation

The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements to prepare for and respond to cyber security incidents in support of maintaining effective CS&IA arrangements.

Inspectors should consider the dutyholder's ability to demonstrate compliance with their security plans through the exhibition of behaviours and knowledge, and the provision of evidence. This may include:

Incident Management

- Check that the organisation has a strategy for identifying and managing all types of security incidents:
  - How do they test this?
- Confirm by questioning appropriate personnel that the dutyholder has a good understanding of the type of incidents that they may face.
- Obtain a copy of the incident management policy and confirm that it coherently and effectively documents their process for identifying and managing incidents.
- Check that the plan is managed and resourced adequately.
- Ensure that the plan is aligned with business continuity and disaster recovery plans.
- Check by questioning that personnel in the organisation understand their responsibilities for incident management.
- Obtain evidence that incidents are logged and reported upon. Inspectors should consider reviewing the organisation's incident log to confirm this:
  - Who do they inform?
  - Is it timely?
- Review evidence of management action in response to incidents.
- Establish that there is an adequate lessons learned process.

The following documents are representative of evidence that may be referenced in the security plan and should be sought for review prior to the inspection:

- Incident management policies.
- Incident management procedures.
- Test and exercise scenarios.
- Business continuity and disaster recovery plans.
- Risk assessments.
- Threat assessments.
- Post incident procedures.
- Test and exercise reports.

12 ANNEX F – TABLE SHOWING THE LINKAGE BETWEEN HMG SPF AND SYAPS

HMG Security Policy Framework		Security Assessment Principles	
Outcome I	**Good Governance**	**FSyP 1**	**Leadership and Management for Security**
Outcome II	**Culture and Awareness**	**FSyP 2**	**Organisational Culture**
Outcome III	**Risk Management**	**FSyP 7** SyDP 7.1	**CS&IA** Effective Cyber and Information Risk Management
Outcome IV	**Information**	**FSyP 7** SyDP 7.2	**CS&IA** Information Security
Outcome V	**Technology and Services**	**FSyP 7** SyDP 7.3	**CS&IA** Protection of Nuclear Technology and Operations
Outcome VI	**Personnel Security**	**FSyP 8**	**Workforce Trustworthiness**
Outcome VII	**Physical Security**	**FSyP 7** SyDP 7.4	**CS&IA** Physical Protection of Information and Information assets
Outcome VIII	**Preparing for and Responding to Security Incidents**	**FSyP 7** SyDP 7.5	**CS&IA** Preparation for and Response to Cyber Security Incidents
Requirement	**III a) Mature understanding of security risks IV a) Staff who are well trained**	**FSyP 3**	**Competence Management**

13 ANNEX G – CS&IA PLAN TEMPLATE FOR R22 DUTYHOLDERS WITH LIMITED SNI

Organisation Details

Organisation	
Organisation Name	
Organisation Head Office Address	

Organisation Locations Where SNI is Held		
	Address	**Highest Level of SNI Held**
Location 1		
Location 2		
Location 3		
Location 4		
Location 5		

Leadership and Management for Security

Responsible Persons			
	Name	Telephone No	Email Address
Chief Executive Officer (or equivalent)			
Board Member responsible for security			
Senior Information Risk Owner (SIRO)			
Chief Information Security Officer (CISO)			
Security Manager			
Internal Regulator			
Crypto Custodian			

CS&IA Governance and Leadership
Describe how your directors, managers and leaders focus the organisation on achieving and sustaining high standards of CS&IA and on delivering the characteristics of a high reliability organisation.

CS&IA Assurance Processes
Describe the CS&IA assurance function within your organisation.

Organisational Culture

Maintenance of a Robust CS&IA Culture
Describe how you develop and maintain a CS&IA culture to ensure the entire organisation recognises that a credible threat exists, CS&IA is important and the role of the individual in maintaining it is key.

Education and Awareness
Describe how the CS&IA policies, procedures and guidance are made available to staff and how changes are communicated.
Describe your CS&IA awareness and training programme for new and existing employees.

Competence Management

Analysis of CS&IA Roles and Associated Competencies
Describe the process of training and measurement which provides confidence that all personnel whose actions have the potential to impact upon CS&IA meet defined competence expectations.

Effective Cyber and Risk Management

Effective Cyber and Risk Management
Describe the risk governance structure within your organisation.
Describe your organisation's CS&IA risk management approach.
Detail your organisational CS&IA risk assessment methodology.
Describe your organisation's CS&IA risk treatment approach.
Explain how residual risks are managed within your organisation.
Have all organisational CS&IA risks been identified?
Have all organisational CS&IA risks been mitigated to a level acceptable to your organisation's risk appetite?

Information Security

CS&IA Strategy, Policy and Standards
Describe the structure of your organisation's CS&IA strategy, policies, procedures and guidance. Provide references for key documents and attach copies or appropriate extracts to this template.

Classification and Control of SNI
Detail how your organisation classifies and controls SNI.

Classified Contracts

Classified Contracts Identification
Describe your mechanisms for identifying and assuring classified contracts.

Contractor Assessment and Assurance
Describe your arrangements for assessing contractors.

Classified Contracts Undertaken
Describe briefly any classified contracts involving SNI that your company is currently undertaking.

Classified Contract Awarded

If you are a Contracting Authority please provide details of all classified contracts where SNI you control is shared

Contractor Company Name	Contractor Site Address	Highest Level of SNI Held	Date of Last Inspection

Protection of Nuclear Technology and Operations

Organisation Digital Assets				
System Name	**Highest Level of SNI**	**Type (Stand Alone/LAN/WAN)**	**Accreditation Authority**	**Physical Location**

Achieving the Cyber Protection System Outcome and Response Strategy
Describe how you have selected the correct CPS outcomes for your organisation's digital assets.
What are the main CS&IA controls for your organisation's digital assets and describe how these are appropriate to meet the CPS outcomes identified above.

Resilience and Assurance of Controls
Detail how you provide resilience and assurance of your system security controls.

Physical Protection of Information and Information Assets

Physical Security Risk Assessment
Describe the process used to determine your office physical security measures.

Physical Security Control Measures
How is entry to your office for authorised personnel controlled? For example, is there a pass system, a PIN system, or keys (or a combination of these)?
Does the office have different security controls for non-business hours? If so, explain the 'out of hours' procedure and what the entry controls are during this period.

Describe any identification that authorised personnel wear within the office.
Describe how visitors gain access to the office - both during the day and 'out of hours' if permitted.
Are security guards used within your office? If so, describe which company they work for, where they are positioned, and what tasks they perform during the day and 'out of hours'.
Does your office have its own alarm system? If so, describe how the alarm is set, how it is known that the office is empty, who can deactivate the alarm, and who responds when the alarm is raised.
Does your office have its own CCTV system? If so, describe where the cameras are positioned, whether are they monitored or recorded (and during what times), where the footage is stored and for how long, and who responds to an incident.
Describe how incoming mail and parcel deliveries are handled from arrival in the building to delivery to the individual's desk.
Describe how outgoing mail and parcels are handled from the individual through to courier or Royal Mail collection.
Describe how facilities management is delivered to the office (e.g. routine maintenance, cleaning arrangements etc.), and whether this is outsourced. Include how facilities management staff gain access to the office and whether they are escorted.
Describe the information storage you use. Include what containers are used, whether access is on a company, project or individual level, and how access is controlled to these. If keys are used please detail how these are secured.
Are PINs or combinations used for access? If so, describe how often they are changed and what happens when a member of staff no longer needs access.
Describe the process for disposing of hard copy information and removable media. Include whether it is shredded or destroyed immediately, stored for batch destruction, or destroyed in another location by a third party company.

Do you use any third party storage or archiving services for SNI? If so, please describe the policy, procedure or guidance for making use of them. Please describe any existing approvals the third party company has and how approval was obtained.

Physical Security Assurance
Describe how you assure your physical security measures.

Preparation for and Response to Cyber Security Incidents

Incident Management
Detail your arrangements for identifying and managing all types of Cyber Security incidents.

Business Continuity and Disaster Recovery (BCDR)
Describe your BCDR arrangements to protect the confidentiality, integrity and availability of SNI.

Cyber Security Incident Assurance
Detail your processes to test and exercise your security incident management and BCDR arrangements.

Incident Reporting

Incident Reporting
Are you aware of your legal obligation to report events and matters under NISR 2003?
Detail your processes and procedures to report such incidents.

Workforce Trustworthiness

Workforce Trustworthiness
Describe how your 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).
Detail how your organisation delivers the appropriate combination of recruitment checks and vetting to satisfy themselves of the honesty and integrity of potential employees.
Describe how your organisation implements and maintains on-going personnel security management, arrangements and procedures to remain assured about your employees and contractors; and to mitigate the risks from well-placed insiders.