1

ONR GUIDE			
INFORMATION SECURITY			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-7.2 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2023
Approved by:	Paul Shanes	Professional Lead (cyber security)	
Record Reference:	CM9 Folder 4.4.2.23373. (2019/135702)		
Revision commentary:	Fit for purpose review of Revision 0		

TABLE OF CONTENTS

Published 03/20

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). 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 (Reference 1).

1.2 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.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgement during assessment activities relating to a dutyholder's 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 dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 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, 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.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2). Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

4.4 The IAEA also publishes Implementing Guide NSS No. 23-G ‘Security of Nuclear Information’ (Reference 8) and Technical Guidance NSS No. 17 ‘Computer Security at Nuclear Facilities’ (Reference 9).

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Security Delivery Principle 7.2 – Information Security, in support of FSyP 7 – CS&IA. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) describes the Cabinet Secretary’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. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 6) indicates those categories of SNI which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 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.

6.2 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 and operational technology (equipment or software). It is a dutyholder's 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. Appendix 1 provides a description of SNI and a flow chart to assist in its identification.

6.3 Information and associated assets may be held by personnel of dutyholders and their supply chain companies and effective CS&IA arrangements should address protection at all times and in all forms.

6.4 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-parties
- Assurance of third-parties
- End of contract

Regulatory Expectations

6.5 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.		

7. INFORMATION ASSURANCE STRATEGY, POLICY AND STANDARDS

Information Assurance Strategy

7.1 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: Effective Cyber and Information Risk Management.

7.2 The scope should include partners, 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.

7.3 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.

7.4 A specific programme for CS&IA (or a similar vehicle) 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 adequate resourcing and support from a communications plan to explain its purpose across the organisation (to include third-parties).

CS&IA Policy and Standards

7.5 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

7.6 Technical CS&IA policy measures are described in more detail in TAG 7.3: Protection of Nuclear Operations and Technology. Further guidance on CS&IA policy aspects is available from a number of sources including:

- HMG (e.g. CPNI, NCSC, CO)
- Nuclear authorities (e.g. ONR, IAEA, IEC, US NRC)
- 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?
  - Is the strategy adequate to identify and manage risks to information and associated assets?
- Does the dutyholder have 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?

8. DATA CLASSIFICATION AND SENSITIVITIES

8.1 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.

8.2 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.

8.3 Annexes F and G to the SyAPs provide a framework for categorising SNI (including Information Technology (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 dutyholder’s classification mechanisms and processes should fit within.

8.4 Dutyholders should create and maintain an Information Asset Register (IAR) or similar mechanism that is an accurate record of what information and associated assets the organisation is responsible for, what format they are in, what value they have and where they are located.

8.5 Dutyholders should consider the use of electronic data labelling or tagging tools to mark and track information and associated assets using metadata.

8.6 The scope of the IAR should include information and associated assets managed by third-parties. 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.

Inspectors should consider:

- Does the dutyholder have a CS&IA strategy that is appropriate to the organisation?
  - Is it adequate to identify and manage risks to information and associated assets?
- Is there a CS&IA policy scoped to the organisation?
  - Does it cover the relevant policy topics adequately?
  - Does it reflect CS&IA relevant good practice?

- 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?

9. IDENTIFICATION OF CLASSIFIED CONTRACTS

9.1 Dutyholders may have contracts with third-parties to provide services to systems operating with SNI on the dutyholders' own sites. The dutyholder's risk management process should include any relevant risks from such service provision (e.g. outsourcing of IT system management).

9.2 Dutyholders may also have contracts with third-parties for services involving SNI on the third-party sites. 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.

9.3 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.

9.4 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. An example of this approach is the Cyber Security Model operated by the Defence Cyber Protection Partnership (see Reference 12).

9.5 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.

9.6 In accordance with the requirements from the Cabinet Office Contractual Process (Reference 13), dutyholders should have a means of alerting companies bidding for contracts for service or goods that a particular contract will involve SNI assets.

9.7 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.

9.8 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.

9.9 The register should also capture details of subcontracts that may involve SNI.

Inspectors should consider:

- Are dutyholders able to clearly identify contracts they have with third-parties that involve information and associated assets?

- Do they have a mechanism for assessing the 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, their sensitivity and how they are to be protected?
    - Is this mechanism used down the supply chain and managed effectively?

10. CS&IA ASSESSMENTS OF THIRD-PARTIES

10.1 Assessing third-party site security 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.

10.2 Dutyholders undertaking their own site survey should consider features from CS&IA methodologies such as: NCSC 10 Steps to Cyber Security, the IASME Cyber Essentials Standard, SANS / CPNI Top 20, NIST Framework, Information Assurance Maturity Model or ISO27001 Annex A 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.

10.3 Dutyholders should have a structured approach to the conduct of third-party assessments. The approach has to 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 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.
- 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 identified to managers and escalated appropriately.
- A process to follow up on identified areas of concern to ensure that they are addressed.

10.4 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:

- 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?
- Is cyber and information risk management in place and effective?

10.5 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: Physical Protection of Information.

Inspectors should consider:

- Are the arrangements used by dutyholders to assess CS&IA maturity for third-party companies adequate?
- Is the scope of the arrangements adequate?
- Do the arrangements manage down the supply chain appropriately?
- Are the arrangements consistent with SyAPs?
- Is there a process for ensuring that any issues identified are reported promptly and addressed?
- Do the arrangements use a structured approach that produces consistent, auditable results that take account of the context of the organisation in scope?

11. ASSURANCE OF THIRD-PARTIES

11.1 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) 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.

11.2 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

11.3 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.

11.4 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.

11.5 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?
- Is it supported by contractual conditions that provide for a response in the event of deficiencies arising?
- 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?

12. END OF CONTRACT

12.1 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.

12.2 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.

12.3 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.

12.4 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 sought from NCSC.

12.5 Dutyholders should ensure that they have an asset management process that identifies when information and associated assets have been returned or destroyed appropriately. 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.

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

13. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

2. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **Classification Policy for the Civil Nuclear Industry.** ONR. http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles for the Civil Nuclear Industry.** ONR. http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

8. **IAEA Nuclear Security Series No. 23-G**. Security of Nuclear Information http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf

9. **IAEA Nuclear Security Series No. 17**. Computer Security at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

10. **NCSC - A Critical Appraisal of Risk Methods and Frameworks** https://www.ncsc.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks

11. **HMG Government Security Classifications.** Cabinet Office https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

12. **Defence Cyber Protection Partnership** https://www.gov.uk/government/publications/defence-cyber-protection-partnership-cyber-risk-profiles/overview-dcpp-and-cyber-security-controls

13. **Contractual Process.** Cabinet Office https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367491/Contractual_Process.pdf

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

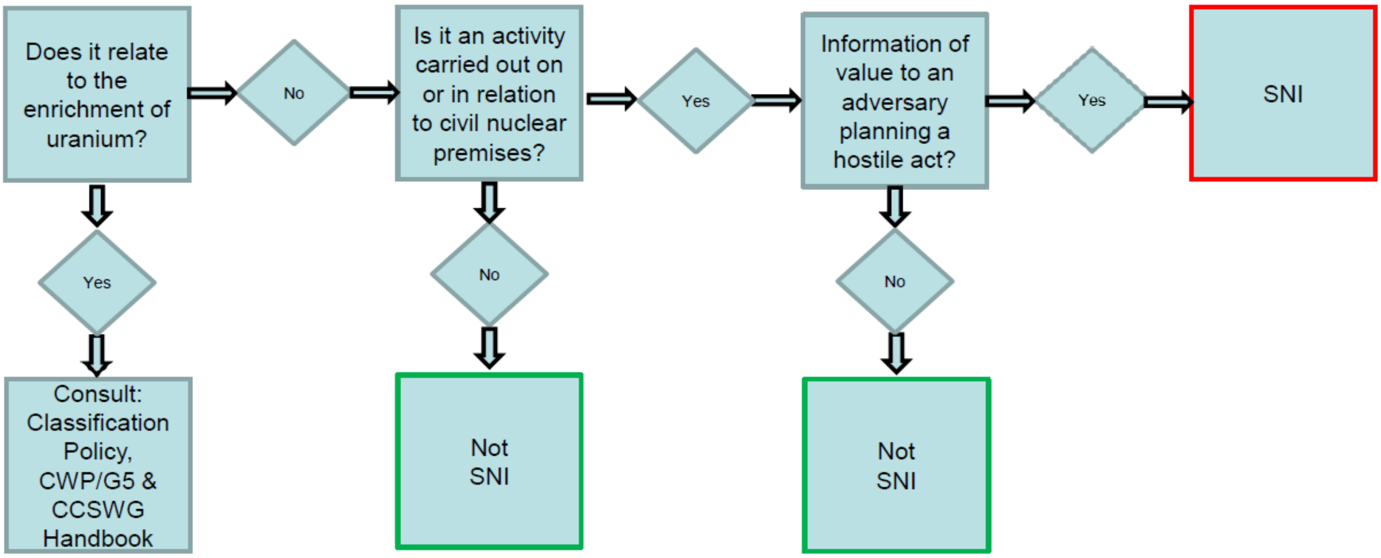
14. GLOSSARY AND ABBREVIATIONS

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
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
IAR	Information Asset Register
IT	Information Technology
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
SNI	Sensitive Nuclear Information
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: IDENTIFICATION OF SENSITIVE NUCLEAR INFORMATION

1. Sensitive nuclear information is information which:

- relates to activities carried out on or in relation to civil nuclear premises; and
- is of value to an adversary planning a hostile act.


Does it relate to the enrichment of uranium?
No
Is it an activity carried out on or in relation to civil nuclear premises?
Yes
Information of value to an adversary planning a hostile act?
Yes
SNI
Yes
Consult: Classification Policy, CWP/G5 & CCSWG Handbook
No
Not SNI
No
Not SNI