Office for
Nuclear Regulation

NISR 2003 – Classification Policy for the Civil Nuclear Industry			
Doc. Type	ONR Policy		
Unique Doc. ID:	ONR-CNSS-POL-001	**Issue No.:**	8.02
Record Reference:	2021/83781		
Date Issued:	Nov-2021	**Next Major Review Date:**	Nov-2026
Prepared by:		Inspector	
Approved by:		Superintending Inspector	
Policy Owner:		Superintending Inspector	
Revision Commentary:	Issue 8.02 – Handling instructions for SNI clarified and updated to reflect current relevant good practice.		

Nuclear Industries Security Regulations 2003

CLASSIFICATION POLICY

For the Civil Nuclear Industry

INFORMATION CONCERNING THE USE, STORAGE AND TRANSPORT OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL

Office for Nuclear Regulation

Published 11/21

CONTENTS

Page

CLASSIFICATION POLICY

General Principles

1. The Nuclear Industries Security Regulations (NISR) 2003 require those who operate within the civil nuclear industry to protect Sensitive Nuclear Information (SNI) in an appropriate manner.

2. SNI is defined in the Anti-terrorism, Crime and Security Act (ATCSA) 2001 (as amended), as including:

- 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.

3. This definition is further amplified in NISR 2003 and The Energy Act (TEA) 2013. ATCSA and TEA share the same basic definition of SNI. NISR defines SNI by reference to ATCSA but adds that SNI includes information that needs protective marking under the ONR Classification Policy. This latter description is reiterated by the notice issued on 25th March 2014 by the Secretary of State under Section 71 of TEA, which states that the following description of information, relating to activities carried out on or in relation to civil nuclear sites, needs to be protected in the interests of national security:

- Information requiring a classification in accordance with either the ONR document 'Classification Policy for the Civil Nuclear Industry', issued on 2nd April 2014, or the ONR and Ministry of Defence document 'ACO 300', issued in January 2002.

4. Whilst not taking precedent over the legal definitions within the statute above, 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 hostile act.

5. The Government Security Classifications (GSC) document[1] details that there is no expectation that routine OFFICIAL information will be marked. SNI is included in the official sensitive subset of OFFICIAL information. This subset covers information that could have more damaging consequences if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but it attracts additional measures to reinforce the 'need to know'. Therefore, OFFICIAL-SENSITIVE assets that contain SNI should be conspicuously marked as below. However, when referring to such assets within a document, it is acceptable to use the abbreviation O-S:SNI.

OFFICIAL-SENSITIVE:SNI

6. Information asset owners may wish to consider applying an appropriate tag to the metadata of digital SNI that enables it to be clearly identified and differentiated from other OFFICIAL-SENSITIVE information that may not be SNI.

Classifying SNI

7. The security classification levels for SNI are: OFFICIAL-SENSITIVE, SECRET and potentially TOP SECRET.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

8. Specific examples for different types of documents and data that may contain SNI are provided in Annex A of this Policy. The following descriptions of consequences should form the basis of judgement when applying a security classification to a specific document:

- SNI that could have damaging consequences if lost, stolen or disclosed without authorisation should be classified as OFFICIAL-SENSITIVE. This relates to sensitive information concerning arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of Nuclear Material (NM)/Other Radioactive Material (ORM) and supporting systems or through the compromise of SNI. It typically applies to less detailed information concerning Category I – III NM or Vital Areas (VAs)[2] that is only likely to affect a single layer of defence in depth and/or be of minimal consequence to the overall security effect. Most sensitive information concerning Category IV NM, ORM, Baseline Areas or protective measures for SNI will also be OFFICIAL-SENSITIVE.
- SNI where compromise could seriously damage nuclear security should be protectively marked SECRET. This relates to very sensitive information concerning arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of NM/ORM and supporting systems or through the compromise of SNI. It typically applies to highly detailed and exploitable information regarding Category I – III NM and VAs which could facilitate attack planning by affecting several layers of defence in depth and/or jeopardising an effective security response. There may also be instances where details of protective measures for SNI are SECRET.

Handling Instructions

9. Standard control measures when working with information assets at each classification level are detailed in GSC. However, it is ONR’s expectation that digital SNI will always be protected by suitable encryption and therefore the additional specific mandatory security controls required for the protection of OFFICIAL-SENSITIVE:SNI within the civil nuclear industry are:

- Electronic information, **at rest** and **in transit**, must be adequately protected by a suitably assured solution[3]. The level of assurance gained will depend upon the assessment scope. Such assessments should take account of recognised principles for product design, security functionality, the asset environment, and specifics of implementation, along with through life assurance in line with guidance set out by the National Cyber Security Centre (NCSC), as the National Technical Authority (NTA).
- Removable Media (USB memory sticks, CD, DVD, external-HDD, floppy disc, etc.) used for SNI data transfer should be encrypted using a suitably assured product in line with NCSC guidance.
- SNI must not be transmitted by fax in the UK or overseas unless its use is required as a standby measure and has been justified and agreed with ONR.

[2] Further detail on the categorisation of NM and VAs can be found in SyAPs Annexes A & B and ONR Technical Assessment Guides 6.1 and 6.2.

[3] If an NCSC assured solution is not available, or its use is not practicable, dutyholders may make a risk-based decision to use an equivalent solution. The associated risk should be escalated and managed as part of your organisation's risk management system.

10. 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 Centre for the Protection of National Infrastructure (CPNI), as the NTA.

International Sharing

11. The international exchange of SNI is a complex area and requirements can vary depending upon the countries involved. As well as the HMG Government Functional Standard GovS 007: Security, GSC and SyAPs, dutyholders must take into account: Cabinet Office guidance for the sharing of Classified Information with international partners; General Security Agreements (where appropriate); and the security requirements of the overseas country concerned. ONR's regulatory expectations are that the Contracting Authority must ensure appropriate protective security controls are in place for the protection of SNI against compromise or loss wherever it is stored, processed, transmitted, controlled, secured or accessed regardless of whether this is in the UK or overseas. Dutyholders should undertake a risk assessment of any such proposed transfers of SNI overseas. Where concerns arise or risks appear unacceptable, dutyholders should seek additional guidance from HMG.

Organisational Classification Guidance

12. The content of this document is not sufficient to be used in isolation by inexperienced staff when applying a security classification to information they produce. Therefore, dutyholders should use this classification policy as a framework to compile their own organisation-specific guidance.

13. The structure of the annex of this classification policy has been aligned with the Security Assessment Principles[4] document. This provides a reference set from which dutyholders should select those elements that are relevant to their particular organisation and operations; for example, content relating to nuclear premises may not be applicable to a location that holds only SNI. However, in all cases it is critical that the descriptions of consequence in this policy are used when interpreting the guidance in the annex.

14. The activities of operating reactors, new build, decommissioning, fuel production and waste sites vary significantly as will the types and security classifications of information produced by them. By selecting the most relevant sections of the annex, dutyholders should be able to develop highly tailored guidance on the application of security classifications that includes specific examples of the types of information generated by their organisation that may contain SNI and the security classification it should be. This highly tailored approach will help ensure that staff are well-trained, can exercise good judgement, take responsibility and are accountable for the information and associated assets they control, including all partner information.

[4] http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

ANNEX A: CLASSIFICATION GUIDANCE

FSYP 1 - LEADERSHIP AND MANAGEMENT FOR SECURITY

SyDP 1.1 - Governance and Leadership

1.1.1 General information relating to governance and leadership, which may include nuclear security policy, management systems, terms of reference, roles and responsibilities, performance management systems etc. Not SNI

SyDP 1.2 - Capable Organisation

1.2.1 General information relating to organisational and nuclear security capability, which may include roles and responsibilities staffing reviews succession planning, staff development budget information etc. Not SNI

1.2.2 SNI relating to organisational capability may include nuclear baseline, security plans, security related documents, security reviews etc:

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 1.3 - Decision Making

1.3.1 General information relating to security decision making, which may include decision makers, processes and information flows etc. Not SNI

1.3.2 SNI relating to decision making may include documents detailing security options, uncertainties, conservatism, detailed operational requirements, concept of operations etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 1.4 - Organisational Learning

1.4.1 General information relating to organisational learning for security, which may include policies, procedures, processes, procedures non-sensitive learning from experience reports etc. Not SNI

1.4.2 SNI relating to organisational learning may include operational experience programmes, security event reports, investigation reports etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 1.5 - Assurance Processes

1.5.1 General information relating to assurance processes, which may include terms of reference, performance Indicators, frameworks, methodologies etc. Not SNI

1.5.2 SNI relating to assurance processes may include detailed evidence-based assurance processes which may include security performance reports, internal inspection reports etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 2 - ORGANISATIONAL CULTURE

SyDP 2.1 - Maintenance of a Robust Security Culture

2.1.1 General information relating to the development and maintenance of a security culture, which may include policies, procedures, information management systems, security education material etc. Not SNI

FSYP 3 - COMPETENCE MANAGEMENT

SyDP 3.1 - Analysis of Security Roles and Associated Competencies

3.1.1 General information related to the analysis of security roles and associated competencies which may include job or task analysis, staffing levels, statements of personnel responsibilities etc. Not SNI

3.1.2 SNI relating to the analysis of security roles and associated competencies may include specific analysis in documents such as security plans, security operating procedures, dutyholder’s nuclear security policy, operational experience feedback etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 3.2 - Identification of Learning Objectives and Training Needs

3.2.1 General information relating to the identification of security learning objectives and training needs, which may include analysis of roles, tasks and competencies, training programmes, training media etc. Not SNI[5]

[5] In the great majority of cases training material will be **Not SNI**. However, there may be specific specialist cases where training material may be of value to an adversary and should be protectively marked. An example may be information relating to Nuclear Power Station training simulators.

SyDP 3.3 - Measurement of Competence

3.3.1 General information regarding the implementation and maintenance of a process of assessment which provides confidence that all personnel whose actions have the potential to impact upon nuclear security meet defined competence expectations., which may include core level competencies, training programme design, evaluation of training effectiveness etc. Not SNI

SyDP 3.4 – Organisation of and Support to the Training Function

3.4.1 General information regarding an organisations' training function for all personnel whose actions have the potential to impact upon nuclear security, which may include training policy, training records, training roles and responsibilities etc. Not SNI

FSYP 4 - NUCLEAR SUPPLY CHAIN MANAGEMENT

SyDP 4.1 - Procurement and Intelligent Customer Capability

4.1.1 General Information regarding procurement and intelligent customer capability, which may include supply chain policy and procedures; generic contractual requirements; quality assurance; arrangements to mitigate the risks of counterfeit, fraudulent and suspect items etc. Not SNI

4.1.2 SNI relating to procurement and intelligent customer capability may include detailed information on arrangements to mitigate the risks of counterfeit, fraudulent and suspect items being introduced; or specifications of nuclear and related equipment items in documents such as security specifications, technical specifications etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 4.2 - Supplier Capability

4.2.1 General information concerning dutyholder due diligence to ensure supplier capability to carry out work with nuclear security significance, which may include quality plans, design, procurement, manufacturing, fabrication and inspection records etc. Not SNI

SyDP 4.3 - Oversight of Suppliers of Items or Services that may Impact on Nuclear Security

4.3.1 General information relating to dutyholders conducting effective oversight and assurance of their supply chain for items or services that may impact on nuclear security, which may include oversight and assurance processes, procurement process arrangements etc. Not SNI

4.3.2 SNI relating to dutyholders conducting effective oversight and assurance of their supply chain for items or services that may impact on nuclear security may include detailed information concerning security arrangements for the protection of SNI in the supply chain in documents such as contracting authority assurance reports, security plans, vulnerability assessments etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 4.4 – Commissioning

4.4.1 General information relating to testing and commissioning, which may include details for handover of responsibilities and acceptance etc. Not SNI

4.4.2 SNI relating to commissioning may include detailed information concerning testing and commissioning any facility, system or process that may affect security, detailed in documents such as risk assessments, drawings, operating and maintenance procedures, security improvement schedules, modification procedures, operating and maintenance manuals, operational requirements, security plans etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 5 - RELIABILITY, RESILIENCE AND SUSTAINABILITY

SyDP 5.1 - Reliability and Resilience

5.1.1 General information regarding the reliability and resilience of security structures, systems and components etc. Not SNI

5.1.2 SNI relating to reliability and resilience may include records indicating mean time between failure, probabilities and/or parameters of detection etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 5.2 - Examination, Inspection, Maintenance and Testing

5.2.1 General information relating to the Examination, Inspection, Maintenance and Testing (EIMT) of security structures, systems and components, which may include plant maintenance schedules, maintenance instructions, quality plans, maintenance records etc. Not SNI

5.2.2 SNI relating to EIMT of security structures, systems and components may include configurations of operational security systems, temporary security plans, vulnerability analysis, risk assessments, inspection reports revealing vulnerabilities, etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 5.3 - Sustainability

5.3.1 General information relating to sustainability of and support to the constituent parts of a nuclear security regime, which may include documented management decisions, funding, succession planning etc. Not SNI

5.3.2 SNI relating to sustainability may include risk assessments, threat assessments, detailed procedures, security performance assessments etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 6 - PHYSICAL PROTECTION SYSTEMS

SyDP 6.1 - Categorisation for Theft

6.1.1 General information relating to the categorisation for theft, which may include the methodology used in order to determine the categorisation for theft, site categorisation, generic locations (e.g. site addresses) of where NM/ORM is in use or storage, accounting principles, aggregated annual NM material balance figures etc. Not SNI[6]

6.1.2 SNI relating to categorisation for theft may include quantity and form together with specific information (e.g. store locations, building numbers) of where Cat I-III NM is in use or storage including waste streams and waste intended for disposal; NM throughput; NM accounting; defence ownership of NM/ORM[7]; and detailed NM balance information etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

[6] Information concerning Euratom Inventory Change Reports, Material Balance Reports and Physical Inventory Listings should be prefixed Eura.

[7] Reference should be made to ACO 300 or Security Aspects letters detailing the classification to be applied under the terms of a contract.

SyDP 6.2 - Categorisation for Sabotage

6.2.1 General information about the methodology used in order to determine the categorisation for sabotage, which may include the International Atomic Energy Agency and ONR Technical Assessment Guide 6.2 definition of a VA, the existence of a VA on a site etc. Not SNI

6.2.2 SNI relating to categorisation for sabotage may include VA identification submissions, the location of a VA on a site, the protective arrangements for a VA; also any information that could identify means whereby individuals(s) acting maliciously can cause a radiological release[8] from a plant such as safety cases, engineering documents and related information etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 6.3 - Physical Protection System Design

6.3.1 General information about physical protection system design, which may include simple details of construction, layout and general references to utilities, easily observable external features etc. Not SNI

6.3.2 SNI relating to physical protection system design may include specific details of construction and layout showing features of physical security relevant to the prevention or theft or sabotage of NM/ORM; reference to utilities that are essential to the functioning of a plant including power supplies for security systems; circuit diagrams or data showing types, configuration and locations of intruder detection system sensors and closed circuit television cameras; and operational procedures covering the intra-site movement of Cat I/II NM or use of NM/ORM stores etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 6.4 - Vulnerability Assessments

6.4.1 General information about vulnerability assessments, which may include the fact the site has undertaken a vulnerability assessment, review processes or initiators, the types of methodology used etc.

6.4.1 SNI relating to vulnerability assessments may include adversary path analysis, attack, delay and response times, any documents pertaining to the protection of NM/ORM where vulnerabilities are revealed etc.

[8] Guidance on what constitutes a significant radiological release (causing unacceptable radiological consequences) is given in the O-S:SNI Annex to SyAPs. The dose thresholds for Baseline and Vital Areas provide a scale on which the appropriate protective marking can be assessed.

i) Sensitive information which could have damaging consequences if the information was lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 6.5 - Adjacent or Enclave Nuclear Premises

6.5.1 General information about adjacent or enclave nuclear premises, which may include procedures for information sharing and maintenance of a coherent, coordinated approach towards all aspects of security (and emergency response). Not SNI

6.5.2 SNI relating to adjacent or enclave nuclear premises may include information detailing the shared security or safety services; or contingency/emergency arrangements between adjacent or enclave nuclear premises.

i) Sensitive information which could have damaging consequences if the information was lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 6.6 - Nuclear Construction Sites

6.6.1 General information about nuclear construction sites, which may include high level project plans, generic designs etc. Not SNI

6.6.2 SNI relating to nuclear construction sites may include details of the physical protection system that ensure its activities cannot be exploited by an adversary to incorporate a latent defect or to pose a threat to an adjacent site.

i) Sensitive information which could have damaging consequences if it was lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 6.7 - Protection of NM During Offsite Transportation

6.7.1 General information about the protection of NM during offsite transportation that does not reveal any potential vulnerability, which may include nuclear train routes, rolling stock details, flask/package design etc. Not SNI

6.7.2 SNI relating to the protection of NM during offsite transportation may include movement information, notifications, security incident reports, high security vehicle data, vulnerabilities of vehicle and vessel tracking systems, design and function of security devices, alarms and immobilisation devices, keys and combination settings for security locks, information on secure communications systems, security plans, security staffing, temporary storage arrangements during transport, and CNC escort arrangements for NM movements.

i) Sensitive information which could have damaging consequences if it was lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 7 - CYBER SECURITY AND INFORMATION ASSURANCE

SyDP 7.1 - Effective Cyber and Information Risk Management

7.1.1 General information about effective cyber and information risk management, which may include CS&IA policies, procedures, risk management communications plans, business objectives, business risk registers, risk appetite statements etc. Not SNI

7.1.2 SNI relating to effective cyber and information risk management may include security risk registers, risk assessments, threat assessments, details of security controls, cyber protection systems.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 7.2 - Information Security

7.2.1 General information about information security, which may include strategies, policies, procedures, asset registers, organisation specific classification guidance etc. Not SNI

7.2.2 SNI relating to information security may include detailed internal or third-party (contract security) assessments, locations of sensitive assets,

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 7.3 - Protection of Nuclear Technology and Operations

7.3.1 General information about protection of nuclear technology and operations which may include system policies, operational technology categorisation processes, Security Operating Procedures, etc. Not SNI

7.3.2 SNI relating to the protection of nuclear technology and operations may include comprise comprehensive documentation which identifies cyber protection systems and be detailed in documents such as Risk Management Accreditation Document Sets (RMADS); Information Technology Health Checks; vulnerability assessments; penetration tests; and firewall rule sets etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 7.4 - Physical Protection of Information

7.4.1 General information about the physical protection of information, which may include policies, procedures, etc. Not SNI

7.4.2 SNI relating to the physical protection of information may include comprehensive physical security risk assessments relating to the protection of SNI, risk assessments, physical protection systems, operational requirements, security plans, Classified Material Assessment Tools, details of security controls etc.

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 7.5 - Preparation for and Response to Cyber Security Incidents

7.5.1 General information to both reduce the vulnerabilities of information and associated assets and to ensure that dutyholders are able to detect and manage cyber security incidents to recover operational functions. This may include incident management policies and procedures, test and exercise scenarios, etc. Not SNI

7.5.2 SNI relating to preparation for and response to cyber security incidents may include business continuity and disaster recovery plans, risk assessments, threat assessments, post incident procedures, test and exercise reports, etc. O-S:SNI

i) Sensitive information which could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 8 - WORKFORCE TRUSTWORTHINESS

SyDP 8.1 – Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security

8.1.1 General information about cooperation of departments with responsibility for delivering screening, vetting and ongoing personnel security. May include internal assurance policies and processes, inter-departmental protocols, exit policies, etc. Not SNI[9]

8.1.2 Personnel records held by dutyholders (which may include sensitive information relating to financial difficulties, medical conditions, the misuse of alcohol or drugs, or criminality). Completed National Security Vetting (NSV) questionnaires. Not SNI[4]

[9] Whilst much personnel security information is not SNI, it is still very sensitive and the Data Protection Act 1998 and common law, under the law of confidence, apply. In addition, although not SNI per se, many such document may still be classified O-S.

SyDP 8.2 - Pre-employment Screening and National Security Vetting

8.2.1 General information about pre-employment screening and NSV, which may include BPSS or NSV record checks, personnel security policies and processes, Baseline Standard Verification Records, Basic Disclosure certificates, police certificates, sworn affidavit or statutory declarations, NSV clearance certificates, Annual Security Appraisal Forms etc. Not SNI[4]

8.2.2 SNI relating to pre-employment screening and NSV material may include information relating to activities carried out on or in relation to civil nuclear premises that needs to be protected in the interests of national security.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 8.3 - Ongoing Personnel Security

8.3.1 General information about ongoing personnel security, which may include Annual Security Appraisal Forms, mandatory notification reports, casualty returns, Change of Personal Circumstances Questionnaires, police reports, medical reports, etc. Not SNI[4]

8.3.2 SNI relating to ongoing personnel security material may include information relating to activities carried out on or in relation to civil nuclear premises that needs to be protected in the interests of national security.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 9 - POLICING AND GUARDING

SyDP 9.1 - CNC Response Force

9.1.1 General information about the CNC Response force in support of the dutyholder that does not reveal any potential vulnerability, which may include total CNC establishment, statutory responsibilities etc. Not SNI

9.1.2 SNI relating to CNC operations in support of the dutyholder may include integrated plans covering tactical and operational policing arrangements, security contingency plans, coordinated policing policies, site specific MOUs, operational procedures, information about the strength and deployment of the CNC; armed response capabilities and timings at a site; and details of CNC firearms holdings and armouries etc.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 9.2 – Local Police Operations in Support of the Dutyholder

9.2.1 General information about the local police operations in support of the dutyholder, which may include statutory responsibilities etc. Not SNI

9.2.2 SNI relating to local police operations in support of the dutyholder may include integrated plans covering tactical and operational policing arrangements, security contingency plans, coordinated policing policies, site specific MOUs, operational procedures etc.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 9.3 – Security Guard Services

9.3.1 General information about security guard services, which may include roles and responsibilities, policies and procedures, resourcing, recruiting, training and equipping etc. Not SNI

9.3.2 SNI relating to security guard services may include security plans, security contingency plans etc.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

FSYP 10 - EMERGENCY PREPAREDNESS AND RESPONSE

SyDP 10.1 – Counter Terrorism Measures, Emergency Preparedness and Response Planning

10.1.1 General information about security contingency measures and response planning, which may include the existence of plans, national threat level, government response level system, media strategy, training policy, training material, etc. Not SNI

10.1.2 SNI relating to security contingency measures and response planning may include sector threat level and threat assessments, CT measures, emergency preparedness and response arrangements to deal with nuclear security events arising on the site and their potential effects, security plans etc:

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 10.2 - Testing and Exercising the Security Response

10.2.1 General information about testing and exercising the security response, which may include security contingency exercise objectives, training programmes, that a site level exercise has been held or is due to take place etc. Not SNI

10.2.2 SNI relating to testing and exercising the security response may include exercise scenarios, security contingency plans; security plans; physical protection system security outcomes; etc.:

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

SyDP 10.3 - Clarity of Command, Control and Communications Arrangements during and Post a Nuclear Security Event

10.3.1 General information about clarity of command, control and communications arrangements during and post a nuclear security event, which may include administrative arrangements, protocols etc. Not SNI

10.3.2 SNI relating to clarity of command, control and communications arrangements during and post a nuclear security event may include security contingency plans, security plans, etc.

i) Sensitive information that could have damaging consequences if lost, stolen or published in the media. O-S:SNI

ii) Very sensitive information where compromise could seriously damage nuclear security. S

ABBREVIATIONS

The following abbreviations are used throughout this policy:

ACO	Atomic Control Office
CNC	Civil Nuclear Constabulary
CPNI	Centre for the Protection of National Infrastructure
FSyPs	Fundamental Security Principles
GSC	Government Security Classifications
NM	Nuclear Material
Not SNI	Not Sensitive Nuclear Information (i.e. information not subject to regulation under NISR 2003)
NTA	National Technical Authority
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material (includes Radioactive Sources)
O-S	OFFICIAL-SENSITIVE
O-S:SNI	OFFICIAL-SENSITIVE:SENSITIVE NUCLEAR INFORMATION
RMADS	Risk Management Accreditation Document Sets
S	SECRET
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
SNI	Sensitive Nuclear Information
VA	Vital Area