|  |
| --- |
|  |
| ONR Policy  The Nuclear Industries Security Regulations 2003: Classification policy for the civil nuclear industry |



ONR Policy

The 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*

**Policy Owner** – Technical Director

**Authored by** – Nuclear Security Inspector

**Approved by** – Head of Profession for Cyber Security and Information Assurance

**Issue:** 9

**Published:** October 2024

**Next scheduled review:** October 2029

**Document reference:** ONR-CNSS-POL-001

**Record reference:** 2021/83781

Revision commentary:

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 9 | General additions and updates in line with the revised Government Security Classification Policy, ONR Security Assessment Principles (SyAPs), and relevant good practice. Updated document template. |

Contents

[Purpose 4](#_Toc180403432)

[Scope and applicability 5](#_Toc180403433)

[Classifying and protecting SNI 6](#_Toc180403434)

[Identifying and marking SNI 7](#_Toc180403435)

[Security controls 9](#_Toc180403436)

[International sharing 10](#_Toc180403437)

[Regulatory reporting requirements 10](#_Toc180403438)

[Organisational classification guidance 11](#_Toc180403439)

[Appendix - Classification guidance 12](#_Toc180403440)

[References 31](#_Toc180403441)

# Purpose

The Nuclear Industries Security Regulations 2003 (NISR 2003) [1] require Responsible Persons to maintain standards, procedures and arrangements that ensure the security of Sensitive Nuclear Information (SNI) as detailed in a security plan approved by ONR. Similarly, Approved Carriers are required maintain standards, procedures and arrangements that ensure the security of SNI as detailed in a transport security statement approved by ONR. Any other person to whom Regulation 22 applies is required to maintain such 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 SNI. The regulations define SNI to be information which requires a protective marking, in accordance with this classification policy.

The purpose of this classification policy is to indicate those categories of SNI that require protection and the level of classification to be applied. It is to be implemented in conjunction with HM Governments (HMG) Government Security Classifications Policy (GSCP) [1] and Government Functional Standard GovS 007: Security [2].

This classification policy is supported by an appendix, which provides non-prescriptive guidance on the types of documents that may or may not contain SNI. Together, the classification policy and guidance provide a framework for dutyholders to compile their own detailed organisation-specific classification scheme as part of an overarching programme of information assurance driven by the board.

# Scope and applicability

SNI is defined in the Anti-terrorism, Crime and Security Act (ATCSA) 2001 [4] (as amended), 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.

The ATCSA definition is referenced in NISR 2003 [1] which additionally highlights that SNI requires a protective marking in accordance with this classification policy.   
The ATCSA definition is also reflected in the Energy Act 2013 (TEA13) [5] and amplified to include information ‘of any description’ relating to activities carried out on or in relation to ‘civil nuclear premises’[[1]](#footnote-2). 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.

# 

# Classifying and protecting SNI

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse). The GSCP provides an administrative system for HMG and partners to protect information assets appropriately against prevalent threats [2]. The administrative system uses three classification tiers: OFFICIAL, SECRET and TOP SECRET. Protective security controls and baseline behaviours when working with information assets at each classification level are detailed in the GSCP [2]. These controls represent HMGs minimum expectations for the protection of information.

Additional assurance is required to protect SNI and meet ONR expectations in ONR Security Assessment Principles (SyAPs) [6] and compliance with NISR 2003.   
The security classification levels for SNI are OFFICIAL, SECRET and potentially TOP SECRET.

The need to comply with this policy, which should be considered to be relevant good practice for the industry, arises from a requirement within NISR 2003.

# 

# Identifying and marking SNI

GSCP guidance indicates that in most cases there are limited to no negative consequences if OFFICIAL information is compromised.

SNI in the OFFICIAL tier uses the -SENSITIVE marking as the implications of a compromise[[2]](#footnote-3) could be potentially significant. It carries the additional sector specific ‘SNI’ descriptor to identify it as a category of information with special sensitivities which invites additional controls.

The GSCP provides recommended baseline behaviours and measures associated with verbal, hard copy and electronic information for OFFICIAL information marked -SENSITIVE which are designed to reinforce the ‘need to know’ principle [2].

SECRET information is much more sensitive than OFFICIAL information and its compromise has potentially serious implications. Consequently, it requires enhanced protective controls, the use of appropriately assured IT and heightened user discretion to guard against compromise. This is reflected in the GSCP enhanced security baseline behaviours and controls [2].

The information creator is responsible for assessing the potential impact of a compromise of information and the expected threat profile to determine whether information is SECRET. Handling and security requirements must be clearly communicated to recipients, and all recipients must have a clear need-to-know. When marking SNI assets the following must be observed:

* OFFICIAL-SENSITIVE assets that contain SNI should be conspicuously marked as OFFICIAL-SENSITIVE:SNI. When referring to such assets within a document, it is acceptable to use the abbreviation O-S:SNI.
* SNI at the SECRET and TOP SECRET level does not require the ‘SNI’ descriptor.
* In the UK, SNI relating to gas centrifuge technology will also bear the ATOLL caveat. ATOLL data retains legacy security markings from the UK's Government Protective Marking System (GPMS). Accordingly, SNI bearing the ATOLL caveat will be marked RESTRICTED, CONFIDENTIAL or SECRET.
* In line with the GSCP, all SNI sent to foreign governments or international organisations (for example, the North Atlantic Treaty Organisation (NATO)) must be marked with a UK prefix. Additionally the UK prefix should be applied in circumstances where a dutyholder identifes a requirement to share SNI overseas in accordance with international sharing arrangements and guidance in the GSCP [2].

Information asset owners (IAOs) 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.

Should there be any queries related to other legacy arrangements or documentation, including those specific to defence procurement and classification of information, dutyholders should seek guidance from ONR.

Further guidance in the form of generic examples for different types of documents and data that may contain SNI are provided in the appendix 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 cause no more than moderate damage if compromised 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)[[3]](#footnote-4) 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 threaten life (an individual or group) or seriously damage the UK’s national or nuclear security should be 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/II 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. Whilst not an exhaustive list, the following categories of information should be subject to control and carriage at the SECRET level:
  + Whole or part references taken from content in the Design Basis Threat (DBT) marked as SECRET.
  + Vital Area Identification submissions and studies where Vital Areas have been confirmed.
  + Security Vulnerability Assessments which details vulnerabilities or deficiencies in security that could be exploited for malicious purposes concerning Category I/II NM and/or Vital Areas.

# Security controls

Standard control measures when working with information assets at each classification level, including specific guidance around the aggregation and classification of information, are detailed in supporting guidance to the GSCP [7]. 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[[4]](#footnote-5). The level of assurance gained will depend upon the assessment scope. Such assessments should take account of recognised principles for product design, security functionality, data sovereignty, the asset environment (including Cloud and digital service providors), 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) for information assurance and cyber threats.
* Removable media (i.e., 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.
* 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 National Protective Security Authority (NPSA), as the NTA for physical and personnel protective security.

# 

# International sharing

The international exchange of SNI is a complex area and requirements can vary depending upon the countries involved. As well as the GSCP [2], GovS 007 [3] and the SyAPs [6], dutyholders must take into account:

* guidance from HMGs Cabinet Office 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 in consulation with ONR as the competent security authority.

‘The Handbook’, issued by the Centrifuge Collaboration Security Working Group (CCSWG), contains specific expectations for dutyholders dealing with the international transfer of SNI which bears the ATOLL caveat [8].

# Regulatory reporting requirements

Regulations 10, 18 and 22 of NISR 2003 require dutyholders to report to the ONR any event or matter including any theft, loss or unauthorised disclosure, of SNI, or any suspected such theft, loss or disclosure. Such reporting is to be undertaken as soon as practicable, and in any event within 24 hours of your organisation becoming aware of the event. A follow-up written report is to be submitted to ONR by means of an INF1 form [9].

# Organisational classification guidance

Dutyholders should review their information and classification policies and remind staff of regulatory expectations for the protection of SNI in order to meet the challenges of the home/remote working environment.

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 detailed organisation-specific classification scheme. They should remind staff of regulatory expectations to meet the challenges of home/remote working.

The structure of the appendix in this policy has been aligned with the SyAPs [6].   
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 appendix.

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 appendix, 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 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 and are competent to handle such information.

# Appendix - Classification guidance

**Note for authors of classification schemes**

The following guidance is intended to assist authors of classification schemes to identify documents that may contain SNI and support the establishment of mechanisms and processes to ensure assets are properly classified in accordance with this policy and are appropriately protected.

This appendix reflects an outcome-focused regulatory framework that sets out the principles with which dutyholders are required to comply and does not constrain dutyholders to a prescriptive set of instructions. It is intentionally high-level and is intended to be used by dutyholders for the development of their own detailed classification schemes tailored to meet their operations and inventories.

The main criteria to be used in assigning specific classifications is the policy in the main document, repeated here:

* For information at OFFICIAL-SENSITIVE:SNI, this typically applies to less detailed information concerning Category I – III NM or Vital Areas (VAs)[[5]](#footnote-6) 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.
* For information at SECRET it typically applies to highly detailed and exploitable information regarding Category I/II 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.

ONR remain available for the provision of advice and guidance to support the development of classification schemes.

| FSyP 1 – Leadership and Management of Security | | Classification |
| --- | --- | --- |
| 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: |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (for example, if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

|  |  |  |
| --- | --- | --- |
| FSyP 2 – Organisational Culture | | Classification |
| 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 – Management of Human Performance | | Classification |
| --- | --- | --- |
| SyDP 3.1 – Identification and Analysis of Security Tasks and Roles | | |
| 3.1.1 | General information related to the identification and analysis of security tasks and roles which may include policies, methodologies and procedures, roles, and responsibilities for conducting analyses of tasks. | Not SNI |
| 3.1.2 | SNI relating to specific tasks important to nuclear security and the ways in which they are undertaken. Metrics which identify the relative importance of specific tasks and roles that deliver security functions. Information drawn from the analysis of tasks important to security that identifies potential routes to human error and the failure to deliver security functions. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 3.2 – Sufficiency and Competence of Persons Delivering Security | | |
| 3.2.1 | General information related to the identification of required staffing numbers, organisation and competency for staff delivering tasks. This may include policies, processes and methods of analysis including activity, task and workload analysis. The general arrangement of the competence assurance function and the methods employed to systematically analyse tasks in order to identify training needs and the associated planning, conduct and assessment of training and trainees. | Not SNI[[6]](#footnote-7) |
| 3.2.2 | SNI deriving from the specific analysis of staffing and competence management arrangements including, detailed role descriptions, staffing numbers, organisation of staffing and chains of command. Training and competence assessment materials that reveal details of how tasks important to security are undertaken and how they contribute to the delivery of security functions. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 3.3 – Suitable and Sufficient Workspaces, Equipment and User Interfaces | | |
| 3.3.1 | General information related to the methods to be employed to ensure, workspaces, equipment and user interfaces necessary for the delivery of security functions are designed to maximise human reliability and minimise the likelihood of human error. This may include policies, processes, methods and standards to be used in the identification of user requirements for the design and/or procurement of workspaces, equipment and user interfaces. | Not SNI |
| 3.3.2 | SNI deriving from the specific analysis of user requirements including identification of key parameters, equipment and human interfaces where compromise could lead to the failure to deliver safety or security functions. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 3.4 – Suitable and Sufficient Procedures and Administrative Controls | | |
| 3.4.1 | General information related to the methods for the production, verification, validation, use and management of procedures and other documents that control the way in which tasks important to security are undertaken. | Not SNI |
| 3.4.2 | SNI relating to specific information that provides details of how tasks important to security are undertaken, this could include security operating procedures. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 4 – Nuclear Supply Chain Management | | Classification |
| --- | --- | --- |
| 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 5 – Reliability, Resilience and Sustainability | | Classification |
| --- | --- | --- |
| 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 6 – Physical Protection Systems | | Classification |
| --- | --- | --- |
| 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[[7]](#footnote-8) |
| 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[[8]](#footnote-9); and detailed NM balance information etc. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| 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 definition of a VA [10], 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[[9]](#footnote-10) from a plant such as safety cases, engineering documents and related information etc. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. | Not SNI |
| 6.4.2 | 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 6.7 – Protection of NM During Offsite Transportation[[10]](#footnote-11) | | |
| 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 Civil Nuclear Constabulary (CNC) escort arrangements for NM movements. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 7 – Cyber Security and Information Assurance | | Classification |
| --- | --- | --- |
| 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 7.2 – Information Security | | |
| 7.2.1 | General information about information security, which may include strategies, policies, procedures, 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, information asset registers, and the location of sensitive assets. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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 comprise comprehensive documentation which identifies cyber protection systems and be detailed in documents such as Operational Technology risk assessments, Information Technology Health Checks, vulnerability assessments, penetration tests, firewall rule sets, system configuration, and network topology diagrams etc.[[11]](#footnote-12) |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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, physical protection systems, operational requirements, security plans, Surreptitious Threat Mitigation Process (STaMP) assessments, identification of single points of failure, details of security controls etc. |  |
|  | Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
|  | Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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 |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 8 – Workforce Trustworthiness | | Classification |
| --- | --- | --- |
| SyDP 8.1 – Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security[[12]](#footnote-13) [[13]](#footnote-14) | | |
| 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 |
| 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). | Not SNI |
| SyDP 8.2 – Pre-employment Screening and National Security Vetting | | |
| 8.2.1 | General information about pre-employment screening and NSV, which will 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 |
| 8.2.2 | SNI relating to pre-employment screening and NSV material that may include information relating to activities conducted on or in relation to civil nuclear premises that needs to be protected in the interests of national security. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |
| SyDP 8.3 – Ongoing Personnel Security | | |
| 8.3.1 | General information about ongoing personnel security, which may include Aftercare Incident Reports, Annual Security Appraisal Forms, mandatory notification reports, Change of Personal Circumstances Questionnaires, police reports, medical reports, etc. | Not SNI |
| 8.3.2 | SNI relating to ongoing personnel security material may include information relating to activities conducted on or in relation to civil nuclear premises that needs to be protected in the interests of national security. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 9 – Policing and Guarding | | Classification |
| --- | --- | --- |
| 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S |

| FSyP 10 – Emergency Preparedness and Response | | Classification | |
| --- | --- | --- | --- |
| 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: |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI | |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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.: |  |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI | |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or 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. |  | |
| Sensitive information which could cause moderate damage if unintentionally disclosed or compromised (e.g. if lost, stolen or published in the media). | O-S:SNI | |
| Very sensitive information where compromise could threaten life (an individual or group) or seriously damage the UK’s national or nuclear security. | S | |

# References

|  |  |
| --- | --- |
| [1] | HM Government, “The Nuclear Industries Security Regulations 2003,” 2003. [Online]. Available: https://www.legislation.gov.uk/uksi/2003/403/contents/made. |
| [2] | HM Government, “Government Security Classifications Policy,” 5 August 2024. [Online]. Available: https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html. |
| [3] | HM Government, “Government Functional Standard GovS 007: Security,” 13 September 2021. [Online]. Available: https://www.gov.uk/government/publications/government-functional-standard-govs-007-security. |
| [4] | HM Government, “Anti-terrorism, Crime and Security Act 2001,” 2001. [Online]. Available: https://www.legislation.gov.uk/ukpga/2001/24/contents. |
| [5] | HM Government, “Energy Act 2013,” 2013. [Online]. Available: https://www.legislation.gov.uk/ukpga/2013/32/contents. |
| [6] | ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry (Version 1),” 2022. [Online]. Available: https://www.onr.org.uk/media/g05fszjn/security-assessment-principles.pdf. |
| [7] | HM Government, “Guidance 1.5 - Considerations for Security Advisors,” 5 August 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/66a3799cab418ab055592db8/Guidance\_1.5\_\_Considerations\_for\_Security\_Advisors\_2024.docx\_\_2\_.pdf. |
| [8] | CCSWG, The Collaboration On Gas Centrifuge Technology – Handbook On Security Of Classified Information, 2023. |
| [9] | ONR, “Notify ONR,” [Online]. Available: https://www.onr.org.uk/notify-onr.htm. |
| [10] | ONR, “CNS-TAST-GD-6.2 - Categorisation for Sabotage”. |
| [11] | ONR, “CNS-TAST-GD-6.1 - Target Identification for Theft”. |
| [12] | ONR, “CNSS-SEC-GD-001 - Nuclear Transport Security Guidance for Class B Approved Carriers’,” March 2024. [Online]. Available: https://www.onr.org.uk/operational/other/cnss-sec-gd-001.pdf. |

1. ‘Civil nuclear premises’ means a civil nuclear site, or other premises on which nuclear material is used or stored which are not controlled or operated wholly or mainly for defence purposes.   
   ‘Civil nuclear site’ means a nuclear site other than one controlled or operated wholly or mainly for defence purposes (TEA13, Part 3, Chapter 1, Section 70(3) [5]). [↑](#footnote-ref-2)
2. The accidental or deliberate violation of confidentiality, loss of integrity, or loss of availability of an information object. [↑](#footnote-ref-3)
3. Further detail on the categorisation of NM and VAs can be found in Annexes A and B of the SyAPs [6] and in ONR’s Technical Assessment Guides on ‘Target Identification for Theft’ [7] and ‘Categorisation for Sabotage’ [8]. [↑](#footnote-ref-4)
4. If a 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. [↑](#footnote-ref-5)
5. Further detail on the categorisation of NM and VAs can be found in Annexes A and B of the SyAPs [6] and in ONR’s Technical Assessment Guides on ‘Target Identification for Theft’ [7] and ‘Categorisation for Sabotage’ [8]. [↑](#footnote-ref-6)
6. 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. [↑](#footnote-ref-7)
7. Information concerning Euratom Inventory Change Reports, Material Balance Reports and Physical Inventory Listings should be prefixed Eura. [↑](#footnote-ref-8)
8. Reference should be made toSecurity Aspects Letters detailing the classification to be applied under the terms of a contract. [↑](#footnote-ref-9)
9. Guidance on what constitutes a significant radiological release (causing unacceptable radiological consequences) is given in the O-S:SNI Annex in the SyAPs [6]. The dose thresholds for Baseline and Vital Areas provide a scale on which the appropriate protective marking can be assessed. [↑](#footnote-ref-10)
10. ONR Guidance Document ‘Nuclear Transport Security Guidance for Class B Approved Carriers’ provides additional guidance on classifying SNI to aid the development of Transport Security Statements for approved carriers [12]. [↑](#footnote-ref-11)
11. All SNI relating to designs of gas centrifuges and centrifuge plants studied and developed in any of the four countries within the framework of The Treaties of Almelo and Cardiff (agreements for the isotopic enrichment of uranium) should be also caveated ATOLL, in accordance with the Centrifuge Classification Guide (CWP/G.5). [↑](#footnote-ref-12)
12. United Kingdom Security Vetting (UKSV) as the Vetting Service Provider, and a Department of Cabinet Office is pre-eminent in relation to the holding of personal data. Information obtained for National Security Vetting (NSV) purposes which is directly input by the vetting applicant or sponsor and stored on the National Security Vetting Solution (NSVS) portal is retained in accordance with the UKSV Privacy Policy (<https://www.gov.uk/government/publications/national-security-vetting-privacy-notice>) and only accessible by ONR and UKSV as joint data-controllers. [↑](#footnote-ref-13)
13. Whilst much personnel security information is not SNI, it is still very sensitive, and the Data Protection Act 2018, common law, under the law of confidence, apply. In addition, although not SNI per se, many such documents may still be classified OFFICIAL-SENSITIVE. [↑](#footnote-ref-14)