Nuclear Industries Security Regulations 2003 – Guidance for Inspectors			
Doc. Type	ONR Guidance Document		
Unique Doc. ID:	CNSS-SEC-GD-002	**Issue No.:**	1
Record Reference:	2022/018499		
Date Issued:	Mar-2022	**Next Major Review Date:**	Mar-2027
Prepared by:		Principal Inspector	
Approved by:		Superintending Inspector	
Process Owner:		Superintending Inspector	
Revision Commentary:	First issue of new document.		

Table of Contents

1. Purpose and Scope

1. **Purpose**: The purpose of this document is to provide advice and guidance to ONR's inspectors on the correct interpretation and implementation of the Nuclear Industries Security Regulations (NISR) 2003 [1]. It reflects operational experience and counsel gained from having worked with the regulations for sixteen years. It shares the same structure as the regulations to aid utility. However, inspectors should note that this document has no legal status in itself (for example, it is not considered to be an Approved Code of Practice for evidential purposes) and in no way supersedes, adds to or modifies the duties placed on regulators and dutyholders by NISR 2003.

2. ONR's Security Assessment Principles (SyAPs) [2] and Technical Assessment Guides (TAGs) are to be used for this purpose and they have been referenced at the appropriate points within this document.

3. The content of this document has also been used to underpin ONR's Regulatory Training.

4. **Scope**: Within the document there is a section for each regulation, supported by annexes where appropriate, defining regulatory interpretation and expectations for that specific part of the regulations. The aim is to use plain English to aid the understanding of the regulations and to describe regulatory interpretations and expectations.

2. Definitions

Table 1: Glossary

Glossary	Description
access control	Means to ensure that access to assets is authorised and restricted based on business and security requirements
adversary	Any individual performing or attempting to perform a malicious act. The term threat is used to refer to a postulated adversary against which security measures are designed, whereas an adversary is active and requires an immediate response.
attack	Any attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
authorised person	A natural or legal person that has been granted an authorisation. An authorised person is often referred to as a "licensee" or "operator".
carrier	Any person, organization or government undertaking the carriage of nuclear material by any means of transport.
civil nuclear premises	A civil nuclear site on which nuclear material is used or stored and premises within a nuclear licensed site, in which for example, a person who is not the licence holder, e.g., a tenant that uses or stores nuclear material/ORM. A nuclear premises also includes other locations where Category I, II or III material is used or stored but excludes premises used for temporary storage during approved transportation. It also can be a civil nuclear construction site on which works are being carried out: (i) by a developer; and (ii) pursuant to the grant or issue of a relevant consent, without which the carrying out of those works would be unlawful.
clearance	A generic term used to refer to screening of employees that includes both pre-employment checks and national security vetting.
competent authority	A governmental organization or institution that has been designated by the State to carry out one or more nuclear security functions.
compromise	The accidental or deliberate violation of confidentiality, loss of integrity, or loss of availability of an information object.
cyber security	The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets.
design basis threat	The attributes and characteristics of potential insider and/or external adversaries, who might attempt malicious acts, against which a physical protection system is designed and evaluated.
dutyholder	A generic term to describe 'a responsible person', 'approved carriers' and 'relevant personnel' as defined in NISR.

Glossary	Description
graded approach	The application of physical protection measures proportional to the potential consequences of a malicious act.
insider	An individual with authorised access to nuclear facilities or nuclear activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined to have an adverse impact on nuclear security.
integrity	The property of protecting the accuracy and completeness of assets (including information).
limited access area	Designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes.
nuclear material	Material listed in the table on the categorization of nuclear material, including the material listed in its footnotes, in Section 4 of IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).
nuclear security	The prevention and detection of and response to, theft, sabotage, unauthorised access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.
physical protection	Measures (including structural, technical and administrative protective measures) taken to prevent an adversary from achieving an undesirable consequence (such as radiological sabotage, or unauthorised removal of nuclear or other radioactive material in use, storage or transport) and to mitigate or minimise the consequences if the adversary initiates such a malicious act.
physical protection system	An integrated set of physical protection measures intended to prevent the completion of a malicious act.
protected area	Area inside a limited access area containing Category I or II nuclear material and/or sabotage targets surrounded by a physical barrier with additional physical protection measures.
radioactive material	Nuclear material, as defined in the CPPNM; radioactive sources, as defined in the Code of Conduct for the Safety and Security of Radioactive Sources and other radioactive substances containing nuclides which undergo spontaneous disintegration (a process accompanied by the emission of one or more types of ionizing radiation, such as alpha and beta particles, neutrons and gamma rays).
radiological dispersal device	A device to spread radioactive material using conventional explosives or other means.

Glossary	Description
response level	The level of security required to be in force at sites in response to the currently assessed threat of terrorist action. The Government uses a three-level system (NORMAL, HEIGHTENED AND EXCEPTIONAL) to articulate the Response Level in force across the Civil Nuclear Industry.
risk	The potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences
sabotage	Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.
security classifications	OFFICIAL, SECRET and TOP SECRET are standard terms used to convey the appropriate levels of protection required for SNI and assets.
security contingency plan	A part of the security plan or a stand-alone document that identifies reasonably foreseeable security events, provides initial planned actions (including alerting appropriate authorities), and assigns responsibilities to appropriate operator personnel and response personnel.
security regime	The security standards, security procedures and security arrangements set out in the approved security plan and applied by the operator for the protection of the site and of any plant, equipment or nuclear material or ORM thereon, or nuclear material in transit.
sensitive nuclear information	Information relating to, or capable of use in connection with, the enrichment of uranium, or information of a description for the time being specified in a notice under section 71 of the Energy Act 2013.
tenant	Company or its employees who lease premises on a site.
threat	The product of adversary motivation, intent and capability.
vulnerability	A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat, or, weakness of an asset or control that can be exploited by a threat.

Table 2: Acronyms and Abbreviations

Abbreviations	
ATCSA	Anti-terrorism, Crime and Security Act. (2001)
BPSS	Baseline Personnel Security Standard
CNC	Civil Nuclear Constabulary
CNS	Civil Nuclear Security
CNSS	Civil Nuclear Security and Safeguards

Abbreviations	
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	Design Basis Threat
EMM	Enforcement Management Model
GCBC	Guidance for Class B Carriers
HEU	High Enriched Uranium
HMG	Her Majesty's Government
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
IRD	Improvised Radiological Device
IT	Information Technology
LEU	Low Enriched Uranium
NED	Nuclear Explosive Device
NIA	Nuclear Installations Act (1965)
NISR	Nuclear Industries Security Regulations (2003)
NM	Nuclear Material
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
OUC	Operational Unit Commander
PIDS	Perimeter Intrusion Detection System
PPS	Physical Protection System
RASyP	Regulatory Assessment of Security Plans
SNI	Sensitive Nuclear Information
SPA	Standards, Procedures and Arrangements
SyAPs	Security Assessment Principles
TAG	Technical Assessment Guide
TEA	The Energy Act (2013)
TptSP	Transport Security Plan
TSA	Temporary Security Arrangement
TSP	Temporary Security Plan
TSS	Transport Security Statement

3. Forward

5. Following 9/11, the international community recognised the need to better coordinate efforts to combat the modern terrorist threat. As a consequence, on 28 September 2001, the United Nations Security Council unanimously adopted Resolution 1373 to reaffirm its unequivocal condemnation of the attacks and to put in place wide-ranging, comprehensive steps and strategies to combat international terrorism. One aspect was to call on all states to establish national legislation that would enable the ratification of all existing fifteen international conventions on terrorism. Two of these conventions of particular relevance to the UK's nuclear security framework are the Convention on the Physical Protection of Nuclear Material (CPPNM); and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT).

6. The CPPNM was adopted on 26 October 1979 and was opened for signature on 3 March 1980. Since its entry into force on 8 February 1987, the CPPNM now has more than 140 States Parties. To this day it remains the only internationally, legally binding undertaking in the area of the physical protection of nuclear material. The purposes of this Convention are 'to achieve and maintain worldwide effective physical protection of nuclear material used for peaceful purposes and of nuclear facilities used for peaceful purposes; to prevent and combat offences relating to such material and facilities worldwide; as well as to facilitate co-operation among States Parties to those ends.' The convention was amended in 2005.

7. The International Convention for the Suppression of Acts of Nuclear Terrorism (Also known as 'The Nuclear Terrorism Convention') entered into force on 7 July 2007. It is primarily an international criminal law instrument that defines certain acts as criminal offences and obliges States Parties to establish their jurisdiction over such offences, to render them punishable under their domestic law and to provide for extradition or prosecution of alleged offenders under the principle of 'aut dedere aut judicare' (either extradite or prosecute). In addition to expectations for creating criminal offences, Article 8 states 'For purposes of preventing offences under this Convention, State Parties shall make every effort to adopt appropriate measures to ensure the protection of radioactive material, taking into account relevant recommendations and functions of the International Atomic Energy Agency (IAEA). Within the UK, the legislative and regulatory framework provided by The Energy Act (TEA) 2013 [3], the NISR 2003 and the Office for Nuclear Regulation (ONR) Security Assessment Principles ensures that this international expectation is fulfilled.

8. Also of relevance is UN Security Council Resolution 1540, adopted under Chapter VII of the Charter of the United Nations on 28 April 2004. This resolution places a legal obligation on States to refrain from supporting by any means non-State actors that attempt to acquire, use or transfer nuclear, chemical or biological weapons and their delivery systems.

9. In the late 1990s, it was recognised that the civil nuclear industries' regulatory framework was not as robust as it should be and that the security regulator for the civil nuclear industry lacked independence because it was effectively part of an organisation that it regulated. Consequently, the Office for Civil Nuclear Security was formed in October 2001 as an independent security regulator within the then Department of Trade and Industry. At the same time, work was initiated to improve the legislative basis on which it conducted its regulatory activity. The aim of this work was to produce a modern, comprehensive and effective regulatory system for civil nuclear security. NISR has been revised on several occasions to ensure that they remain up to date. References to NISR in this document are inclusive of all amendments.

10. This improved legislative basis was achieved with the enactment of the NISR 2003 under the Anti-terrorism, Crime, and Security Act (ATCSA) 2001. NISR 2003 created criminal offences for non-compliance and expanded scope to cover the protection of civil nuclear licenced sites and any other premises holding Category I-III quantities of civil nuclear material; transport security of Category I-III quantities of nuclear material; and sensitive nuclear information wherever it is held in the UK. TEA 2013 established the ONR as the UK competent authority for regulating civil nuclear security. As part of this change, NISR 2003 was moved from ATCSA to become a relevant statutory provision of TEA 2013 to support ONR's nuclear security purposes, although ATCSA retains some links to UK civil nuclear security. Together, TEA 2013 and NISR 2003 form the backbone of UK's civil nuclear security, legislative and regulatory framework in compliance with international counter-terrorism instruments.

4. Introduction

11. The Office for Nuclear Regulation (ONR) published the SyAPs [2] in 2017. The principal aim of SyAPs is to provide consistency and guide regulatory judgements and recommendations when undertaking assessments of dutyholders' security submissions, such as site security plans and transport security statements. Underpinning the requirement for these submissions, and ONR's role in their approval, are the legal duties placed on organisations subject to NISR 2003.

12. The SyAPs provide the essential foundation for the introduction of outcome focussed regulation for all constituent security disciplines: physical; personnel; transport; and cyber security and information assurance. This regulatory philosophy is aligned with our mature non-prescriptive nuclear safety regime and provides dutyholders with a coherent regulatory approach applied by ONR across the UK civil nuclear industry.

13. ONR introduced the NISR 2003 Guidance Document in 2003 and subsequently revised the document in 2014. This guidance document was intended to provide plain English advice to dutyholders on the interpretation of NISR 2003 to assist it in maintaining compliance with its requirements. NISR 2003 was originally implemented in a prescriptive fashion to provide clarity, avoid ambiguity and allow for the levels of capability and capacity present within the industry and regulator at the time. Whilst NISR 2003 remains fundamentally unchanged, levels of maturity have improved to allow the adoption of an outcome focussed regulatory regime; this document reflects how NISR 2003 is to be interpreted within this new approach. Furthermore, this guidance document underpins ONR's Regulatory Training.

14. The term 'dutyholder' is used throughout this guide for consistency but reflects any of the following; the 'responsible person' in relation to any nuclear premises as at Regulation 2(2); for Class A and Class B carriers, the 'approved carrier' Regulation 2(1); and in relation to Regulation 22, 'any person who has possession or control of sensitive nuclear information in the United Kingdom' and who is involved in activities prescribed in Regulation 22(1). For accuracy the relevant regulation in NISR 2003 will specify the correct terminology.

15. Regulations 12, 23, 24 have been repealed and are not commented on in this document.

5. Summary of Obligations Under NISR 2003

16. Detailed below is a synopsis of the key obligations under NISR 2003 that inspectors should be aware of:

- The responsible person must submit a security plan to ONR for approval for each nuclear premises for which that person is responsible. Once the plan is approved the responsible person must comply with the Standards, Procedures and Arrangements (SPA) described in the approved security plan for the premises for so long as it remains in force, and any direction given by ONR.

- Thereafter the responsible person may at any time submit to ONR for approval, a fresh security plan for the premises or proposals for amending the approved security plan.

- If it is proposed to carry out any work of alteration or extension to any building or other structure which is, or forms part of, nuclear premises (other than a civil nuclear construction site) and which is not provided for in an existing approved security plan, the responsible person must give notice in writing to ONR in the form of a Temporary Security Plan (TSP).

- The responsible person in relation to each nuclear premises must ensure that each of his relevant personnel have been assessed in accordance with a process that has been approved by ONR, to ensure they are of suitable character and integrity, and having regard to the need to ensure the security of the premises and the material, equipment and information.

- The responsible person in relation to each nuclear premises must report to ONR any event or matter of a kind specified in the regulations **as soon as practicable** and in any event within 24 hours of it becoming known to him.

- There is a requirement for Category I/II nuclear material and Category III nuclear material to be transported by carriers approved by ONR; this approval can be revoked by ONR if requested by the carrier or where there are grounds for ONR to revoke. As part of the process a Class A or Class B carrier must submit an application to become an approved carrier together with a transport security statement for approval by ONR. Where required a transport security plan must be submitted for approval by ONR.

- Once approved the carrier must comply with the standards, procedures and arrangements described in his approved transport security statement or transport security plan and any direction given by ONR. Furthermore, the approved carrier must report any event or matter of a

kind specified in regulations **as soon as practicable** and in any event within 24 hours of it becoming known.

- A person to whom the sensitive nuclear information, uranium enrichment equipment and software regulation applies must maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within their possession or control.

- If any person fails to comply with any provision of Regulation 4(1), 5, 7, 8, 9, 10, 11, 12, 13, 17, 18, 19, 20, 21, or 22, he shall be guilty of an offence.

- Under legislation the male and female gender can be used i.e., of him / he / his / her / she / hers. NISR refers to the Secretary of State as ‘her’ – since it was Patricia Hewitt at the time.

6. NISR Part 1 - Introductory

17. NISR 2003 provides for the regulation of the civil nuclear industry for security purposes and prescribes certain types of fissile material as "nuclear material" for the purposes of the definition of "nuclear material" in section 76(7) of the Anti-terrorism, Crime and Security Act (ATCSA) 2001. The regulations are in five Parts as follows:

- Part 1 provides for introductory matters.
- Part 2 makes provision about the security of nuclear premises
- Part 3 makes provision about the security of transport of nuclear material.
- Part 4 makes provision about the security of sensitive nuclear information
- Part 5 contains general and supplementary provisions
- Within this document each regulation is replicated in a different font type and italics, followed by the explanatory text.

6.1. Regulation 1 – Citation, Commencement, Revocation and Extent

(1) These Regulations may be cited as the Nuclear Industries Security Regulations 2003.

(2) These Regulations come into force on 22nd March 2003, except that Part 3 and the provisions of Parts 1 and 5 so far as they apply for the purposes of Part 3 come into force on 22nd September 2003.

(3) The Nuclear Generating Stations (Security) Regulations 1996 are hereby revoked.

(4) Subject to paragraph (5), these Regulations extend to Northern Ireland.

(5) Paragraph (3) of this regulation and regulations 3(1) and (2) and 23 do not extend to Northern Ireland (but nothing in this paragraph prevents "nuclear material" in these Regulations from having the same meaning in all parts of the United Kingdom (see regulation 2(1)).

(6) Regulation 24 extends only to Northern Ireland.1

18. This provides that the regulations will commence on 22 March 2003, except for Part 3, and Parts 1 and 5 so far as they apply for the purposes of Part 3,

[1] Regulation 24 revoked by the Energy Act 2013.

which will commence on 22 September 2003. It also revokes the regulations formerly providing for the regulation of the security of nuclear generating stations, the Nuclear Generating Stations (Security) Regulations 1996.

6.2. Regulation 2 - Interpretation: General

19. Regulation 2 sets out the meanings of a number of expressions used in the regulations, which inspectors should understand. Additional clarification and context has been provided to aid interpretation as considered necessary.

(1) In these Regulations, unless the context otherwise requires-

"the 2001 Act" means the Anti-terrorism, Crime and Security Act 2001;

"the 2013 Act" means the Energy Act 2013;

"2001 Act direction" means a direction given by the Secretary of State on or after 1st April 2014 under regulations made under section 77(1) of the 2001 Act;

20. 'The Nuclear Security (Secretary of State Security Directions) Regulations 2018', which were made under section 77(1) of the ATCSA 2001, allow the Secretary of State to issue security directions to civil nuclear industry dutyholders in response to certain types of urgent security threat. It is expected that this power will be used only in exceptional circumstances.

"approved carrier" means a Class A carrier or a Class B carrier

21. Companies wishing to transport Category I-III quantities of nuclear material are required to be approved by ONR. This is achieved through the submission of a Transport Security Statement (TSS) that is assessed against SyAPs and approved where arrangements are judged to be adequate. Class A carriers are approved to transport Categories I-III quantities of nuclear material by the modes specified in the TSS, whereas Class B carriers may only transport Category III quantities of nuclear material.

"approved security plan" means a security plan which has been approved by the ONR under regulation 5 or 6, as amended by any amendments approved under regulation 6, and which has not been revoked (but see regulation 8 (temporary security plans));

22. All nuclear premises as defined under Regulation 2 must comply with the standards, procedures and arrangements within a security plan that is approved by ONR. ONR will approve security plans judged to be adequate against the regulatory expectations in the SyAPs and associated TAGs. Approval of a plan encompasses all the SPA included within, relied upon or referenced from the plan.

"approved transport plan" means a transport plan which has been approved by the ONR under regulation 19;

23. In addition to an approved transport security statement, an approved transport security plan is also required for all transports of Category I/II nuclear material. On occasion depending on the form and nature of the material, transport security plans for transports of Category lll nuclear material may also be selected for sampling by ONR.

> *"approved transport security statement" means a transport security statement which has been approved by the ONR under regulation 16, as amended by any amendments approved under that regulation, and which has not been revoked;*

24. Similar to an approved security plan for nuclear premises, transporters of Category I-III quantities of nuclear material must comply with the SPA within a transport security statement that is approved by ONR. ONR will approve transport security statements judged to be adequate against the regulatory expectations in the SyAPs and associated Technical Assessment Guides, including the Guidance for Class B Carriers.

> *"carrier" means a person undertaking the transport of Category I/II nuclear material or Category III nuclear material, and includes both a carrier for hire or reward and a carrier on his own account;*

25. This confirms that a carrier may be a responsible person undertaking the transport as part of their normal operations; or a haulage company being paid to undertake the transport on the consignor's behalf.

> *"Category I/II nuclear material" has the meaning given in regulation 3(3);*

26. Refers to the relevant entry in the schedule to NISR 2003, a more detailed description of nuclear material categorisation is provided in section 3 below.

> *"Category III nuclear material" has the meaning given in regulation 3(4);*

27. Refers to the relevant entry in the schedule to NISR 2003, a more detailed description of nuclear material categorisation is provided in section 3 below.

> *"Class A carrier" means a carrier approved by the ONR under Part 3 of these Regulations to transport Category I/II nuclear material and Category III nuclear material;*

28. As described earlier.

> *"Class B carrier" means a carrier approved by the ONR under Part 3 of these Regulations to transport Category III nuclear material;*

29. As described earlier.

> *"classification policy" means the classification policy "Information concerning the Use, Storage and Transport of Nuclear and other Radioactive Material" issued by the ONR from time to time;*

30. ONR produces this classification policy [4] which describes consequences that should form the basis of judgement when applying a security classification to a document. It also mandates the handling instructions for information falling within the OFFICIAL–SENSITIVE:SNI tier. It is supported by an annex, which provides additional guidance in the form of specific examples of different types of documents and data that may contain SNI and how it might be classified.

"commencement date" means 22nd March 2003;

31. Refers to the date which NISR 2003 came into force.

"enriched", in relation to uranium, means enriched so as to contain more than 0.711% of uranium-235;

32. 0.711% is the percentage of uranium-235 in natural uranium, the remainder being made up of Uranium -238 (though with trace Uranium - 234). Natural uranium is typically enriched up to 5% Uranium - 235 for use in conventional fuels for nuclear power plants. Regardless of the quantity, unirradiated natural and depleted uranium fall outside of the NISR 2003 schedule and are regulated under different legislation.

"nuclear material" has the meaning given in section 70 of the 2013 Act (as extended under subsection (3) of that section);

33. The 2013 Act defines nuclear material as any fissile material in the form of uranium metal, alloy or compound; plutonium metal, alloy or compound; or any other fissile material prescribed by regulations made by the Secretary of State. For the purposes of NISR 2003, this relates to materials as prescribed by Regulation 3 and the Schedule.

"nuclear premises" means—

(a) a civil nuclear site, other than one in relation to which all nuclear material or other radioactive material that was used or stored has been removed as part of the decommissioning.

34. In accordance with the Nuclear Installations Act (NIA) 1965 [5], the site licensee can apply for de-licensing when they have successfully demonstrated that the site presents 'no harm' to the public because all nuclear and radioactive material has been removed. On de-licensing, the site will also no longer be regulated under NISR 2003 and the security plan can be revoked.

(aa) a civil nuclear construction site on which works are being carried out—

(i) by a developer; and

(ii) pursuant to the grant or issue of a relevant consent, without which the carrying out of those works would be unlawful;

35. When a new generation of stations, to be sited adjacent to existing sites, became a serious prospect, the Government amended NISR to address potential security risks during construction especially given the heavy plant involved in the construction that could pose a threat to the existing site or where latent threats could be introduced during construction. The 2013 amendment to NISR 2003 requires nuclear construction sites that are within 5 km of an existing nuclear site to have an approved security plan that details how its operations will be protected to ensure security of the adjacent site is not affected. After site licensing operators are required to have security plans which set out how they will ensure that latent threats are not included.

> *(b) premises that form part of a civil nuclear site and are premises on which a person, who is not the holder of the nuclear site licence and is not acting as an officer, employee or contractor of that holder, uses or stores nuclear material or other radioactive material;*

36. This relates to tenants operating on a civil nuclear site that is involved in commercial activities not relating to that site. Tenants defined as separate nuclear premises may hold a different nuclear site licence or operate under the wider site licence. In either case, they are considered to be separate NISR 2003 dutyholders and each is required to have a distinct approved security plan, albeit making reference to appropriate claims on the arrangements provided by the wider site licence holder. A company other than the licensee operating a facility containing nuclear material / ORM that is used solely in the interests of the licensee, (e.g., dosimetry services) is not considered to be a separate nuclear premise and is therefore not required to have a distinct approved security plan (refer to Paragraph A.36).

> *(c) other civil nuclear premises on which Category I/II nuclear material or Category III nuclear material is used or stored, but excluding premises that are used solely for the purpose of the temporary storage of such material during the course of or incidental to its transport in any case where the standards, procedures and arrangements in respect of the security of the transport are contained in an approved transport security statement;*

37. There are certain nuclear activities that fall outside of the requirement for a nuclear site licence under the NIA 1965 but that may require the use of nuclear materials falling within Category I-III as specified in the schedule to NISR 2003. In these instances, the dutyholder will be required to have an approved security plan for these nuclear materials but it is not a legal requirement under NISR 2003 for the plan to detail the standards, procedures and arrangements to ensure the security of Category IV nuclear material or other radioactive material. The security of these materials other than at licensed sites, where it is regulated by NISR 2003, is regulated under separate legislation by different competent authorities (Health and Safety Executive (HSE) / Health and Safety Executive for Northern Ireland (HSENI) for IRR17 and devolved Environment Agencies under Environmental Protection Regulations 2016 (EPR16), (EAR18), RSA93 and HASS05).

However, the dutyholder may wish to produce and operate under a single security plan that will satisfy all relevant security legislation.

"nuclear site licence" has the same meaning as in section 1 of the Nuclear Installations Act 1965;

38. Section 1 of the NIA 1965 describes the type of activity for which a nuclear site licence is required and makes it an offence for such activity to be undertaken unless a licence has been granted. All civil nuclear licensed sites are also nuclear premises under NISR 2003.

"the ONR" means the Office for Nuclear Regulation;

39. Self-Explanatory.

"relevant personnel", in relation to a person ("the principal") who is the responsible person in relation to any nuclear premises, a carrier or a person to whom regulation 22 applies, means—

(a) each of the principal's officers, employees, contractors and consultants, and;

(b) each officer, employee, contractor or consultant of the principal's contractors and consultants;

40. This makes clear that the term 'relevant personnel' includes any officer or employee of the principal and any employees of companies throughout the extended supply chain (i.e., contractors and any sub-contractors).

"responsible person" has the meaning given in paragraph (2);

41. Further information relating to the interpretation of responsible person is provided at paragraphs A1.30, A1.31, A1.35 and A1.36.

"security plan" must be construed in accordance with regulation 4(2) and (3);

42. The contents of the security plan must cover the specific elements of regulation such as 'any equipment or software used or stored on the premises in connection with activities involving nuclear material'.

"transport" means transport by any means, but excluding—

(a) ***[revoked]***

(b) transport within nuclear premises or between adjacent nuclear premises;

43. Arrangements for intra-site transportation, or between adjacent sites, should be covered in the approved security plan.

"transport plan" must be construed in accordance with regulation 19(3);

44. The contents of the transport plan must cover the specific elements of Regulation 19 such as 'the loading or unloading of the material during the course of or incidental to the transport'.

"transport security statement" must be construed in accordance with regulation 16(2) and (3);

45. The contents of the transport security statement must cover the specific elements of Regulation 16 such as the security of 'any Category I/II nuclear material or Category III nuclear material transported or to be transported by the carrier'.

"United Kingdom person" has the meaning given in section 74(6) of the 2013 Act;

46. TEA 2013 defines a "United Kingdom Person" as:

(a) an individual who is—

(i) a British citizen, a British overseas territories citizen, a British National (Overseas) or a British Overseas citizen,

(ii) a person who under the British Nationality Act 1981 is a British subject, or

(iii) a British protected person within the meaning of that Act,

(b) a Scottish partnership, or

(c) a body incorporated under the law of any part of the United Kingdom.

47. Therefore, a person can be an individual, a Scottish partnership or a corporate body. For a nuclear premises that is a civil nuclear licenced site, section (2) below is clear that the responsible person is the holder of the site licence. Section 3(1)(a) of The Nuclear Installations Act 1965 states that a nuclear site licence may be granted only to a body corporate. Therefore, the responsible person for a civil nuclear licenced site is the body corporate rather than a British citizen. For consistency, the responsible person in relation to tenants on civil nuclear licenced sites, other nuclear premises holding Category I-III quantities of nuclear material and civil nuclear construction sites is also regarded to be the body corporate. Similarly, in relation to transport, the approved carrier (i.e., the person referred to in Regulation 13) is to be regarded as the body corporate. Regulation 22 refers to "any person who has possession or control of sensitive nuclear information", again to maintain consistency it is ONR's policy that this refers to the body corporate.

48. Notwithstanding the policy above, there may be some circumstances where it is appropriate for action to be taken against an individual. Section 102 of

Chapter 5 of TEA 2013 places an obligation that 'Every employee, while at work, must co-operate with any person (whether or not the employer) on whom a requirement is imposed by or under any relevant provision so far as necessary to enable the requirement to be complied with' and it is an offence if an individual does not meet this obligation. Therefore, where an employee is considered to have been grossly negligent or wilfully disregarded expectations (e.g., security policy, practice or work instruction) placed on them by their employer then ONR may consider enforcement action against the individual. However, it should be noted that Regulation 22 also allows prosecution of individuals in possession or control of sensitive nuclear information and this route may be more appropriate depending on advice provided by legal counsel.

"uranium enrichment equipment" means equipment capable of being used in or in connection with the enrichment of uranium;

49. This typically refers to centrifuge technology used to enrich uranium, although other technologies also exist such as gaseous diffusion, which would also be covered.

"uranium enrichment software" means any software capable of being used in or in connection with the enrichment or uranium.

50. This relates to the software used to operate the enrichment technology.

(1A) For the purposes of sub-paragraph (aa) of the definition of "nuclear premises"—

"developer" means a person who is lawfully entitled to carry out works on a site with a view to its becoming a nuclear site;

"relevant consent" means—

(a) development consent within the meaning of section 31 of the Planning Act 2008;

(b) planning permission—

(i) within the meaning of section 336 of the Town and Country Planning Act 1990;

(ii) within the meaning of section 277 of the Town and Country Planning (Scotland) Act 1997;

(iii) within the meaning of article 2(2) of the Planning (Northern Ireland) Order 1991;

(c) an order under section 14 or 16 of the Harbours Act 1964;

(d) an order under section 1 of the Harbours Act (Northern Ireland) 1970;

(e) an order under section 10 of the Harbours Act (Northern Ireland) 1970.

51. This section was introduced as part of the 2013 amendment and extends the scope of NISR 2003 to include civil nuclear construction sites. The important point to note is that the term civil nuclear construction site is defined in TEA Act 2013 as a site:

(a) on which works are being carried out with a view to it becoming a civil nuclear site, and

(b) which is situated within 5 kilometres of an existing nuclear site;

Therefore, a construction site must be within 5km of an existing civil nuclear licenced site for it to be considered to be a nuclear premises and thus within scope of NISR 2003.

(2) "Responsible person", in relation to any nuclear premises, means—

(a) in the case of a civil nuclear site falling within paragraph (a) of the definition of "nuclear premises", the holder of the nuclear site licence;

(aa) in the case of a civil nuclear construction site falling within sub-paragraph (aa) of the definition of "nuclear premises", the developer;

(b) in the case of premises falling within paragraph (b) of that definition, the person mentioned in that paragraph; and

(c) in the case of premises falling within paragraph (c) of that definition, the person who uses or stores the Category I/II nuclear material or Category III nuclear material on those premises, but this is subject to paragraph (3).

52. As described in the section above on "United Kingdom Person", the responsible person in relation to any nuclear premises is considered to be the body corporate rather than an individual citizen.

(3) No person is the responsible person in relation to any nuclear premises falling within paragraph (b) or (c) of the definition of "nuclear premises" by virtue of using or storing nuclear material or other radioactive material on behalf of another person if he is that other person's officer, employee or contractor.

53. This provides clarification that where a body corporate or individual is using nuclear or radiological material on a nuclear premises solely to fulfil a contract with the responsible person of that premises, then the responsible person remains the contracting authority and a separate security plan is not required. An example might be where a licensee has contracted the provision of dosimetry services. The contractor may be the sole occupant of a building containing NM/ORM on the civil licenced nuclear site, but provided their operations are limited to fulfilling the contract for the licensee, the licensee

remains the responsible person. It also specifically excludes an individual (officer, employer or contractor of the licensee) as being considered the responsible person.

(4) For the purposes of paragraph (b) of the definition of "sensitive nuclear information" in section 77(7) of the 2001 Act, information which appears to the ONR to be information which needs protecting in the interests of national security includes information which requires a protective marking in accordance with the classification policy.

54. See reference to the Classification Policy [4].

6.3. Regulation 3 – Meaning of "nuclear material", "Category I/II nuclear material" and "Category III nuclear Material"

55. This section should be read in conjunction with the schedule to NISR 2003 which specifies categories of nuclear material. The table in this schedule is based on the table in Annex II to the CPPNM (though there are some minor differences), which grades nuclear material according to its attractiveness to fashion a Nuclear Explosive Device (NED). It is not appropriate to use this table as the basis of grading materials for attractiveness to fashion an Improvised Radiological Device (IRD) (including both radiological dispersion devices and radiological exposure devices) or an act of direct sabotage. For the former, categorisation is conducted against SyAPs Annex A tables 3 and 4; and Table 1 of Annex B for the latter. Further advice and guidance on the categorisation of nuclear material, other radioactive material and associated facilities can be found in [6] and [7].

(1) For the purposes of paragraph (b) of the definition of "nuclear material" in section 76(7) of the 2001 Act (meaning of "nuclear material" in section 76) material of the following kinds is prescribed—

(a) previously separated americium-241 which is not irradiated,

(b) previously separated americium-242m which is not irradiated,

(c) previously separated americium-243 which is not irradiated, and

(d) previously separated neptunium-237 which is not irradiated.

56. These elements are very rarely encountered in large quantities (generally subcategory III) but nevertheless, they are fissile and have a critical mass similar to that for Uranium - 235. Accordingly, the weights determining the categorisation thresholds for these materials are the same as that for Uranium - 235. The term irradiated is explained below.

(2) In paragraph (1)—

"irradiated", in relation to any kind of material, means that the material has a total radiation output giving a dose rate exceeding 1 Gray per hour at one metre from the unshielded surface of the material; and

57. Where nuclear material meets the criteria for "irradiated", it generally results in a lower categorisation than when it is "unirradiated". The rationale for this is that the high dose rate introduces significant challenges to those wishing to use it to develop a NED because without large amounts of shielding, exposure to that material would cause mortal injury within a relatively small amount of time. Further information on considerations of categorising irradiated materials is provided in [6].

"previously separated", in relation to any kind of material, means that the material has been subject to treatment that increases the concentration of the material.

58. For example, plutonium, americium and neptunium that have been extracted from wider fission products present in spent fuel by means of the solvent extraction process.

(3) For the purposes of these Regulations, nuclear material is "Category I/II nuclear material" if and only if it is—

(a) a kind of nuclear material specified in column 1 of the Table in the Schedule to these Regulations in relation to which there is an entry in column 2 of that Table specifying a quantity (including "any quantity") for material of that kind, and

(b) of such a quantity as is specified in column 2 of that Table for material of that kind.

59. Category I refers to types and quantities of nuclear material that require the least effort to fashion into a nuclear explosive device. The lower thresholds (2kg Plutonium or Uranium - 233; 5kg Uranium - 235 in Highly Enriched Uranium (HEU), Americium or Neptunium) are intentionally set significantly below the critical mass required to generate a nuclear explosion. When determining the categorisation of uranium, it is the weight of Uranium - 235 in combination with the enrichment that are the determining factors.
For example, 10kg of uranium enriched to 80% Uranium - 235 would be a Category I quantity (10 x 0.8 = 8), whereas 10kg of uranium enriched to 30% Uranium - 235 would be Category II (10 x 0.3 = 3).

60. Category II is the maximum categorisation for any quantity of uranium enriched to less than 20% Uranium - 235. It can also refer to smaller quantities (i.e., subcategory I, refer to the schedule for exact masses) of Highly Enriched Uranium (HEU), Uranium 0233, Plutonium, Americium or Neptunium. However, these types, forms and weights are rare within the UK nuclear industry. Instead, Category II tends to refer to spent fuel that is destined for international travel, irradiated material that was Category I prior to

irradiation (e.g., spent mixed oxide fuel or fast reactor fuel) or bulk quantities of waste containing fissile material such as plutonium and HEU.

61. Within the UK, fresh fuel for the current generation of power stations consists of Low Enriched Uranium (LEU) up to 5% enrichment, which is Category III prior to irradiation where the weight of U235 is in excess of 10kg. However, plutonium is produced within the fuel as it burns to the extent that typically, over 200kg of spent fuel would contain sufficient plutonium to place it in Category I. However, it is placed within Category II because of its reduced attractiveness due to the high radiation levels associated with spent fuel and the associated challenges that this poses to machining or processing.

62. This document has already described that categorisation is driven by the attractiveness of the material to fashion a NED. Factors such as dilution, dispersion, type and form can all affect the attractiveness of nuclear material because an adversary will have to acquire much larger volumes and masses of material to obtain a significant quantity of nuclear material and / or undertake additional processes to extract it. In certain circumstances, materials may be categorised in accordance with Table 2 of Annex A to SyAPs (refer to [6] for more information on the applicability of Table 2). Category II is the maximum categorisation within this table in recognition of the reduced attractiveness and there are many facilities within the UK that store bulk quantities of waste resulting from legacy operations (e.g., weapons and research) that fit within this criterion.

> *(4) For the purposes of these Regulations, nuclear material is "Category III nuclear material" if and only if it is—*
>
> > *(a) a kind of nuclear material specified in column 1 of the Table in the Schedule to these Regulations in relation to which there is an entry in column 3 of that Table specifying a quantity (including "any quantity") for material of that kind, and*
> >
> > *(b) of such a quantity as is specified in column 3 of that Table for material of that kind.*

63. This regulation makes it clear that only certain types of nuclear material, and then only if above certain threshold masses, attract a categorisation for theft of Category lll. Category III quantities of material form the majority of site inventories across the UK nuclear industry and are encountered in a range of types and forms. The most common relate to low enriched uranium in the form of uranium hexafluoride (colourless, odourless gas at room temperature and pressure that facilitates centrifuge enrichment), fresh LEU fuel and spent fuel being stored or processed with the UK. Other commonly encountered category III materials include Uranium or Plutonium in sources or arising from storage of fuel element debris. Most other materials that meet the "irradiated" criteria are also considered to be Category III with the exception of irradiated nuclear material that was Category l prior to irradiation.

64. Category III material is unsuitable for fashioning a nuclear explosive device without significant further processing or acquisition of multiple (>4x) quantities. Processing would either require enrichment or building a rudimentary pile to burn the uranium fuel to breed plutonium for subsequent separation. Both of these activities are extremely difficult. As described above, it is the weight of Highly Enriched Uranium - 235 in combination with the enrichment that is the determining factor when categorising uranium that may fall within Category III.

65. All other types and quantities of nuclear materials not listed in the schedule to NISR 2003 are considered to be Category IV and are, therefore, not subject to regulation under NISR 2003 where they are being stored or processed in a location other than a civil licenced nuclear site. Whilst not an exhaustive list, such materials include natural uranium, depleted uranium and thorium.

> *(5) In determining the quantity of material of any kind for the purposes of paragraphs (3)(b) and (4)(b)—*
>
> *(a) in the case of material used or stored on nuclear premises, the quantities of all material of the kind in question that is being used or stored on the nuclear premises in question are to be aggregated, and*
>
> *(b) in the case of material being transported by road, train, ship or air, the quantities of all material of the kind in question that is being transported in the road convoy, on the train, on the ship or in the aircraft, as the case may be, are to be aggregated.*

66. When determining the categorisation of nuclear material stored on a nuclear premises or being transported then the aggregated total of the material is to be used. This total determines whether the material falls within scope of NISR 2003, and if so, the security outcomes that need to be achieved. However, the aggregation is only applicable to materials of “the kind in question”, which means that it is not applied across different elements, isotopes or enrichments. For example, a nuclear premise’s inventory or transport package consisting of 3 sources of uranium enriched to 80% 235, each weighing 10 grammes would be aggregated resulting in a category III quantity (10g x 0.8 x 3 = 24g) and would be subject to regulation under NISR 2003. Conversely, a site inventory or transport package consisting of a 10 gramme plutonium source, a 10 gramme uranium source enriched to 80% U235 and an americium source would not be aggregated resulting in a category IV quantity and would not be subject to regulation under NISR 2003.

7. NISR Part 2 – Security of Nuclear Premises

7.1. Regulation 4 – Requirement for Approved Security Plan for Nuclear Premises

67. This regulation sets out the need for an approved security plan to be in place at all times which describes the standards procedures and arrangements to ensure the security of the elements specified within this regulation and which are applicable to the dutyholder. It further describes a number of key aspects that require additional and specific consideration: vetting; movement of nuclear material; equipment and software used in connection with activities involving nuclear material / ORM; policing and guarding and contingency plans and exercising. Finally, it covers the consideration of threats posed to existing sites by plant and machinery being used during construction of an adjacent site.

> *4(1) The responsible person must ensure that there is an approved security plan in place at all times for each nuclear premises in relation to which that person is responsible (whether or not the premises form part of other premises to which this paragraph applies).*

68. The dutyholder submits their first security plan for approval under Regulation 5 and subsequent replacement, amendments and revocation through Regulation 6. The statement - 'whether or not the premises form part of other premises to which this paragraph applies' -refers to tenants who are licensees or dutyholders in their own right and resident on another nuclear licenced site.

> *4(2) A security plan must describe in writing the standards, procedures and arrangements adopted or to be adopted by the responsible person to ensure the security of—*

69. The statement 'or to be adopted by the responsible person' in paragraph 2 allows for a plan to be approved on the understanding that identified gaps in compliance or regulatory expectations are managed and closed out to agreed specifications and timelines recorded in the plan. ONR has previously expected a 'Security Improvement Schedule' to manage these gaps; under SyAPs the dutyholder may define their own terminology for the process of recording and delivering what has 'to be adopted'. Whatever the process is termed, it must be specified within the security plan to ensure legal compliance. The inspector should consider if the data recorded is sufficient to allow effective management of the activity through to completion (e.g., date issue raised; agreed date for completion and the specifications of the work to be undertaken). Any proposed amendment to this data would require ONR's approval under the dutyholder's change arrangements; see Regulation 6 of this guidance.

4(2)(c) any equipment (or software) used or stored on the premises in connection with activities involving nuclear material,

70. Equipment or software includes both operational technology (OT) (e.g., Industrial control systems and plant such as cranes and fuel charging machines) and information technology (IT) (e.g., Databases and intranets). Software is an essential element required to safely operate OT through systems such as supervisory control and data acquisition (SCADA) and must also be suitably protected to ensure confidentiality, integrity and availability. There is a degree of crossover between OT / IT and SNI. For example, SCADA, particularly security management systems, are comprised of OT (e.g., turnstiles and active hostile vehicle mitigation (HVM)), IT and SNI (recorded CCTV images of controlled areas, or an access control system connected to a networked database with SNI). The scope of 'in connection with activities involving nuclear material' is broad and could be interpreted to include all equipment and software within the site perimeter. ONR takes a proportionate approach and has developed a table at Annex G of SyAPs, which describes the types of equipment and software where regulatory attention will be targeted, together with a categorisation scheme that allows the application of a graded approach to mirror that in place for the protection of nuclear material / ORM.

4(2)(d) any sensitive nuclear information kept on the premises,

71. All sensitive nuclear information should be identified and classified in accordance with the ONR NISR 2003 Classification Policy [4]. The definition is very broad and could include communications between industrial control systems. However, it typically refers to the written word both in hard copy and digital forms whilst in use, storage or transmission. In addition to defining SNI and its appropriate classification, the classification policy mandates the handling instructions for the protection of SNI at the OFFICIAL-SENSITIVE level (referred to as OFFICIAL- SENSITIVE:SNI), which exceed the government baseline expectations. SNI above this classification is protected in accordance with the HMG Government Security Classifications document [8].

72. Regulation 4(2)(e) refers specifically to a nuclear premises or a tenant on an existing nuclear site.

4(3) In particular, but without prejudice to the generality of paragraph (2), the plan must describe the standards, procedures and arrangements relating to—

(a) the investigation and assessment by the ONR of the suitability of relevant personnel of the responsible person with a view to ensuring the security of the premises and the material, equipment and information mentioned in paragraph (2);

(b) the receipt and despatch of any Category I/II nuclear material and Category III nuclear material to be transported to or from the nuclear premises;

(c) the manner in which the nuclear premises are to be policed and guarded, including the identity of the person providing any constables or persons acting as guards, the total number of constables and such persons attached to the premises and the number of such constables or other persons who will normally be present there; and

(d) the steps to be taken by the responsible person or any person acting on his behalf if any event of a kind specified in [regulation 10(5)(a), (b), (e), (f), (g) or (h)] that requires immediate action occurs, and the regular practice of the activities required in connection with those steps.

73. Section 3(a) refers to the pre-employment checks and vetting arrangements that are covered under Regulation 9 and other mandatory requirements.

74. Section 3(b). It is anticipated that the dutyholder's arrangements for recording the receipt and despatch of nuclear material is likely to be detailed within a number of documents to meet ONR's purposes. ONR would not expect this information to be repeated verbatim within the security plan, but to be referenced as supporting documentation. Inspectors should familiarise themselves with all of ONR's purposes to ensure intervention activity and dutyholder arrangements are appropriately integrated.

75. Inspectors should be aware that with regard to section 3(c), ONR's expectation is that the title of the Chief Constable CNC and / or the provider of guarding services is mentioned in the plan. Furthermore, NISR 2003 stipulates that the total establishment and shift numbers required to deliver, and maintain, the necessary operational effect and outcomes are specified in or referenced from the plan. ONR must approve any proposed amendment to these numbers; see Regulation 6 of this guidance. It is also expected that minimum staffing numbers for CNC and / or guards, are specified in the Nuclear Baseline or equivalent document.

76. Section 3(d) refers to the dutyholder's Regulation 10 event response and contingency arrangements, which are normally articulated in the Nuclear Security Contingency Plan (or equivalent), but to include all these arrangements within the wider plan would be burdensome. However, given this legal requirement, the Nuclear Security Contingency Plan must be referenced within the plan.

77. The 'regular practice of the activities required in connection with those steps' refers to the regime that the dutyholder implements to train personnel and test the efficacy of the nuclear security contingency plans to ensure that the required effect and outcome can be delivered on a consistent basis. 'Regular practice' should be judged by inspectors in a proportionate manner considering the risk and potential consequence. This training and exercising regime must be referenced in the wider plan if it is not specified within the Nuclear Security Contingency Plan.

4(3A) Further, and without prejudice to the generality of paragraph (2) —

78. This part of Regulation 4 forms part of the 2013 amendment to NISR 2003 to reflect concern principally of the threats posed to the existing site by the plant and machinery on an adjacent construction site. The two sub paragraphs below achieve the same effect but refer to different phases of construction (i.e., subparagraph (a) refers to a construction site post licensing and subparagraph (b) refers to a construction site pre-licensing).

> *(a) in the case of a [civil nuclear site] (A) which is located within 5 kilometres of a [civil nuclear site] (B), the plan in relation to site A must also describe the standards, procedures and arrangements to ensure the security of site B [in relation to any] activity which is or is to be carried out at site A that may or will affect the security of site B;*

79. In subparagraph (a) above, site A refers to the construction site once it has been licensed but has no nuclear fuel on it, and site B is the existing site.

> *(b) in the case of a [civil nuclear construction site] falling within sub-paragraph (aa) of the definition of "nuclear premises" , which is located within 5 kilometres of a nuclear site, the plan in relation to the [civil nuclear construction site] site must also describe the standards, procedures and arrangements to ensure the security of that nuclear site, [in relation to any] activity which is or is to be carried out at the [civil nuclear construction site] that may or will affect the security of that nuclear site .*

80. In subparagraph (b) above, the civil nuclear construction site is termed as such rather than being a civil nuclear site to reflect that it is not yet licensed however, in both instances the sites can be termed civil nuclear premises.

81. To assist in defining an outcome focussed security plan the following is offered and is based upon the definition within SyAPs:

- A security plan should be a logical and hierarchical set of documents that describes risk in terms of the categorisation for theft and sabotage of the facility or site and the modes of operation, potential vulnerabilities, and those security measures that need to be implemented to prevent or mitigate them. It should demonstrate that the physical protection system achieves the required security outcome and can be operated and maintained in a secure manner. It takes account of experience from the past and sets expectations and guidance for the processes that should operate in the future if security is to be delivered successfully. Under outcome focussed regulation there is an expectation that the security plan clearly articulates the standards, procedures and arrangements through the linkage of security claims, arguments to evidence.

- Under SyAPs the approved security plan consists of the written submission that has the claims, arguments and evidence (i.e., the SPA) articulated within, or referenced from it. The standards, procedures and arrangements referenced from the approved security plan also form part of that plan and are consequently regulated in accordance with ONR's vires. To summarise, all standards, procedures and arrangements that

contribute towards any aspect of security in the approved plan are subject to regulation. Where evidence gaps are identified in the security plan, an amendment should be submitted to address the shortfall.

- The dutyholder should have processes for managing changes (amendments) to standards, procedures and arrangements and these processes should be articulated or referenced in the approved plan. Amendments are approved under Regulation 6.

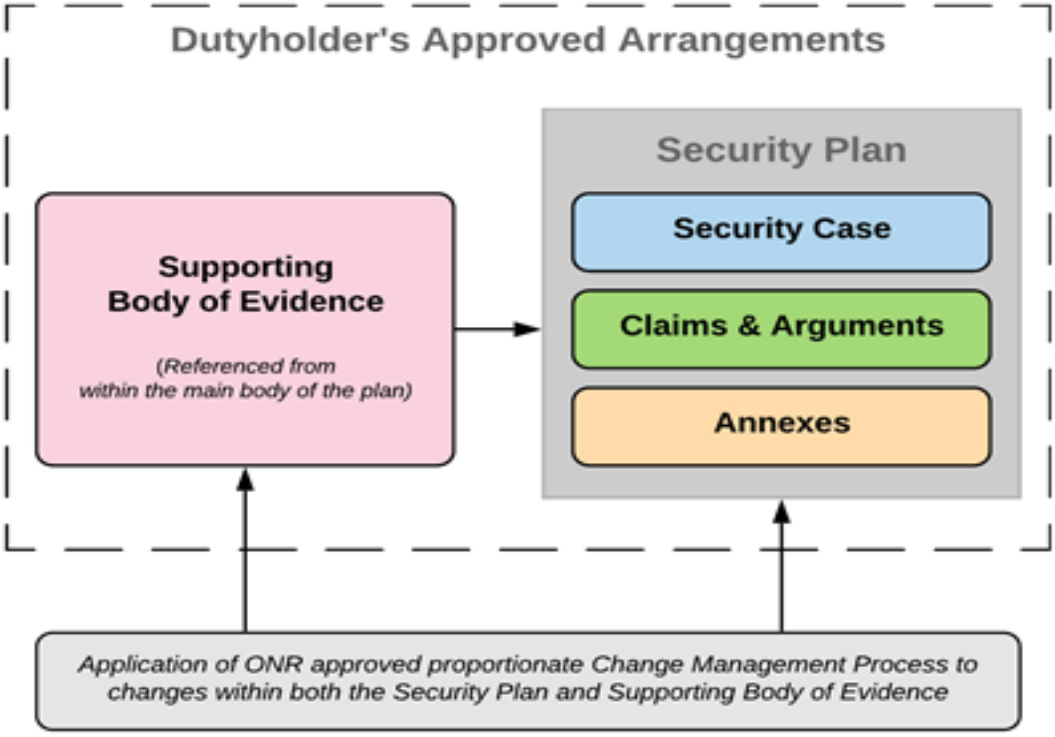

Figure 1: Diagrammatical Illustration of Dutyholder's Approved Arrangements

7.2. Regulation 5 – Submission and Approval of First Security Plans

1) The responsible person in relation to each nuclear premises must submit a security plan for the premises to the ONR for approval.

2) The ONR may approve the plan as submitted or with such amendments as the ONR may require.

3) In the case of premises which are nuclear premises on the commencement date, the security plan must be submitted by 22nd June 2003.

82. Inspectors should be aware that this regulation places a legal obligation on the dutyholder for a security plan to be submitted for approval for every new

nuclear premise. ONR can approve the plan if the requirements set out in Regulation 4 have been met fully or, if not; require amendments to close identified gaps in regulatory expectations.

83. ONR's formal written approval is in the form of an approval letter and supporting approval certificate.

7.3. Regulation 6 – Replacement, Amendment and Revocation of Approved Security Plans

84. Inspectors should be aware that this regulation requires that the approved plan remains current and reflects the SPA adopted or to be adopted by the responsible person to ensure the security of elements specified in Regulation 4(2). ONR's approval of a security plan effectively freezes all the SPA explicitly detailed within, relied upon, or referenced by, the plan. This can create excessive regulatory burden and limit a dutyholder's ability to quickly respond to changes in threat or operating environment. To address this issue, the regulations provide for a notification to be issued under Regulation 7(2), whereby the dutyholder will not be regarded as having failed to comply with the approved plan if, in ONR's opinion, the deviation is unlikely to be prejudicial to security. The effect of this notification is to provide dutyholders with the flexibility to implement specified changes to SPA without continual recourse to the regulator. Refer to paragraph A2.30 - A2.35 for more guidance.

Regulation 6(1). The responsible person in relation to each nuclear premises may at any time submit to the ONR for approval: –

a fresh security plan for the premises, or

85. **Replacement**: There are a number of reasons why the dutyholder may need to submit a replacement security plan for ONR's approval. These may include major lifecycle or operational changes, particularly those affecting categorisation for theft / sabotage and / or where the claims and arguments are fundamentally different; as a consequence of a significant amendment to the Design Basis Threat (DBT); or as part of a defined periodic review. Security plan maintenance and further examples of why the plan may need to be updated are covered under RASyP 7 in SyAPs.

proposals for amending the approved security plan for the premises.

86. Amendment: A proposed amendment to the approved security plan may consist of changes to SPA explicitly detailed within, relied upon, or referenced by, the plan. A proposed change may be temporary or permanent. Proposed changes to SPA explicitly detailed within the plan can only be implemented once the proposed amendment has been approved by ONR. Once approved, and to reduce burden on the dutyholder, ONR is content for the amendment submission to sit with the plan until the defined periodic review results in a replacement plan being submitted. However, if the

proposed textual amendments are significant and widespread throughout the plan it is likely to be more appropriate if the dutyholder submits a replacement plan from the onset. Indeed, in such cases ONR may seek assurance that the combined effect of the changes has been fully considered. A modular approach to security plan design could assist in the amendment process.

87. The arrangements for amending an approved plan by managing changes to the SPA must be included or referenced within the approved plan. These arrangements should be underpinned by a process to define the potential risk / consequence of the change if inadequately conceived or executed and will be assessed by ONR inspectors using the Managing Changes to the SPA Technical Assessment Guide. This TAG articulates a possible process for identifying the significance of, and managing changes to, SPA. In the example articulated within this TAG, Major, Significant and Minor changes would be submitted to ONR for approval under Regulation 6. These changes include any amendment to SPA explicitly detailed within the plan but may also include SPA relied on or referenced by the plan where the potential impact warrants it. Changes considered to be unlikely to be prejudicial to the security of the premises may be implemented without approval from ONR under a Regulation 7(2) notification as described in the next part of this guide.

88. Categorising changes according to impact in this way not only provides for improved dutyholder flexibility, but also allows ONR to implement a proportionate approach to assessment and approval of a proposed amendment by targeting resource on those changes judged to be of greater potential impact to the security regime. Such an approach is dependent on ONR's confidence in a dutyholder's arrangements to manage change as detailed in, or referenced by, the plan. Inspectors should be aware that some dutyholders, particularly those at sites with very low hazard and risk or are in long term steady state, may find that developing these arrangements are not cost beneficial. In such cases, all proposed amendments to SPA explicitly detailed within, relied on, or referenced by the security plan, must be approved by ONR before they can be implemented.

89. **Temporary Amendments**: There may be occasions when the dutyholder wants to make temporary changes to SPA. Inspectors should have an expectation that the dutyholder's arrangements for managing change referenced in the approved security plan will apply equally to changes of a temporary nature. They should also expect that a dutyholder's submission will include appropriate mitigation measures and an anticipated date for completion which will be applied, or amended by ONR, as part of the approval process. If the completion date requires extension, it will be necessary for the dutyholder to justify the extension, and for ONR to approve the extension. ONR would usually limit temporary changes to a maximum of 12 months, after which a permanent amendment of the security plan should be considered. Otherwise, the amendment will be automatically revoked, and the original SPA must be re-established.

90. An example of a temporary amendment may be alternative vetting or access control arrangements to facilitate an outage on a generating reactor site for the duration of the outage.

91. **Administrative Amendments**: Inspectors should be aware that these are defined as amendments to the submitted and approved security plan; paragraph titles; reference document titles and revisions; minor textual changes that have no impact on the delivery of the security regime or any similar amendment to the written form of the approved security plan. These amendments do not need to be submitted for approval by ONR but are to be recorded in accordance with the dutyholder's document control arrangements and ONR informed on an appropriate basis. The aim is to reduce regulatory burden and ensure proportionality. As with other forms of amendments, ONR inspectors will periodically inspect the dutyholder's arrangements to provide assurance that this option is used appropriately.

> *Regulation 6(2) The ONR may approve the plan or proposals as submitted or with such amendments as the ONR may require.*

92. **Approval**: ONR will assess proposed amendments in a proportionate manner (as informed by regulatory intelligence such as ONR's confidence in the dutyholder's change management processes) and formally approve in writing when content that all risks are being appropriately managed. Where an inspector judges a proposed amendment / change fails to provide sufficient assurance that the required security effect can be achieved, they will formally request in writing any necessary amendments to close identified gaps in regulatory expectations.

93. Formal approval by ONR of a replacement plan, or an amendment / change to SPA, will consist of an approval letter, approval certificate or both.

> *Regulation 6(3) On approving a fresh security plan for the premises, the ONR may revoke the approval of the former plan for the premises.*

94. **Revocation**: Inspectors should be aware that ONR would usually revoke an existing approved plan on approving the fresh security plan. Care must be taken to ensure that the dutyholder has prepared the implementation of new arrangements sufficiently to move seamlessly and without risk from one plan to another. It is suggested that there is a clearly defined date and time for transition between plans specified in the approval letter to ensure that there is no confusion as to which plan the dutyholder must comply with.

95. There may be elements of an existing plan that can transition into a new plan; the Security Improvement Schedule and extant notifications are examples. It is important that these elements are fully considered and reflected in the approval documentation.

7.4. Regulation 7 – Maintenance of Security

1) The responsible person in relation to each nuclear premises must comply with the standards, procedures and arrangements described in the approved security plan for the premises.

2) The responsible person is not to be regarded as having failed to comply with any of those standards, procedures or arrangements by reason of any matter if the ONR has notified the responsible person in writing that that matter, or a matter of its description, is in the ONR opinion unlikely to be prejudicial to the security of the premises and the material, equipment and information mentioned in regulation 4(2).

96. NISR 2003 Regulation 4(1) requires nuclear premises to have in place an approved security plan. Inspectors should be aware that Regulation 7(1) requires a dutyholder to comply with the approved plan for their premises; failure to do so is an offence.

97. However, Regulation 7(2) provides the ability to reduce regulatory burden and implement proportionality by allowing ONR to issue a 7(2) notification to the dutyholder for certain matters that have been defined or described within the dutyholder's processes, and for which ONR is content that these matters are unlikely to be prejudicial to the security of the premises. Consequently, the dutyholder will not have failed to comply with the approved security plan for any matter described in the 7(2) notification.

98. As previously stated in Regulation 6, the arrangements for amending an approved plan by managing changes to the SPA must be included or referenced within the approved security plan. These arrangements should be underpinned by a process to define the potential impact of the change if inadequately conceived or executed. Changes ONR considers not to be prejudicial to the security of the premises under these arrangements will be considered as matters where the dutyholder has not failed to comply with their security plan by implementing without prior approval by ONR. ONR will confirm this with the dutyholder by issuing a Regulation 7(2) notification to that effect.

99. The other occasion where a 7(2) notification can be issued is for events and matters under Regulation 10 (5) (i) and (j) where a significance category of the event has been assigned such that it is considered to be of a kind unlikely to be prejudicial to security or of press interest and, therefore, do not need to be submitted to ONR.

100. For amendment, inspectors should be aware that a dutyholder does not need to rely upon a 7(2) notification provided that all amendments are submitted under Regulation 6(1) to ONR for approval. Similarly, 7(2) notifications will not be necessary where events and matters considered to be of a type not prejudicial to security are described in the approved security plan; or where

the dutyholder accepts full compliance with reporting under Regulation 10 (5) (i) and (j).

101. Where possible 7(2) notifications should be issued along with the approval of a security plan (initial or change). Inspectors should also note that where required, a 7(2) notification will be issued to manage changes to SPA, and a separate 7(2) notification will be issued to manage events and matters under Regulation10 (5) (i) and (j).

102. In summary there is the potential for two 7(2) notifications to be issued covering separate regulatory concerns. The first allows dutyholders to adopt changes to SPA ONR considers not be prejudicial to security of the premises without the need to submit an amendment under Regulation 6. The second allows dutyholders to manage security events and matters of little or no impact on security without making a report to ONR in accordance with Regulation 10 (i) and (j).

103. The appropriate notifications are at Appendix 14.

104. In either case ONR will require confidence in a dutyholders arrangements and processes to support issue of a 7(2) notification. Where this is not the case, all changes to SPA will need to be submitted under Regulation 6(1) and any non-compliance with SPA will need to be reported under Regulation 10 (5) (i). This will also be the default position where a dutyholder opts not to implement processes to support the issue of a 7(2) notification.

7.5. Regulation 8 – Temporary Security Plans during Building Works etc.

(1) If it is proposed to carry out any work of alteration or extension to any building or other structure which is, or forms part of, nuclear premises (other than a civil nuclear construction site falling within sub-paragraph (aa) of the definition of "nuclear premises") and which is not provided for in an existing approved security plan with which the responsible person must comply —

(a) the responsible person in relation to the premises must give notice in writing to the ONR —

(i) specifying the nature of the proposed works, and

(ii) stating whether in his opinion they are likely to involve any derogation from any of the standards, procedures and arrangements described in the approved security plan for the premises, and

(b) the works may not be begun until the ONR has approved a temporary security plan for them.

(2) Paragraph (1) does not apply in the case of any particular work if before the work is begun the ONR has notified the responsible person in writing that that work, or any work of a description that includes that work, is in the ONR opinion unlikely to be prejudicial to the security of the premises and the material and equipment mentioned in regulation 4(2).

(3) To obtain approval of a temporary security plan for any works, the responsible person must submit the plan in writing to the ONR.

(4) The temporary security plan must describe any standards, procedures and arrangements which the responsible person proposes to adopt to ensure the security of the premises and the material and equipment mentioned in regulation 4(2) during the period whilst the works are being carried out.

(5) The ONR may approve the temporary security plan as submitted or with such amendments as the ONR may require.

(6) During the period whilst the works are being carried out, the approved security plan for the premises has effect subject to the approved temporary security plan.

(7) During that period the responsible person must comply with the standards, procedures and arrangements described in the approved temporary security plan.

(8) The responsible person may at any time submit proposals for amending the approved temporary security plan to the ONR, and the ONR may approve the proposals as submitted or with such amendments as the ONR may require.

105. The scope of Regulation 8(1) is very broad, requiring the responsible person to tell ONR in writing whenever any work of physical alteration or extension is planned to any building or structure (including structures, systems or components). This needs to be implemented in a way that is manageable and reduces regulatory burden. Therefore, there is provision for ONR to issue a notification under Regulation 8(2) to limit the scope as defined in this section.

106. Inspectors should be aware that the onus is on the dutyholder to identify such work and notify ONR accordingly, taking account of the time necessary for ONR to undertake assessment and approval. Timeliness is an important element noting that work cannot start until ONR has approved the TSP to cover it.

107. Regulation 8(2) recognises that not all work will affect the security of the premises and material and equipment mentioned in Regulation 4(2). Hitherto ONR has issued a notification as part of the security plan approval process that defined types of work of alterations or extension, stating that any other works falling outside of those definitions were considered in ONR's opinion

unlikely to be prejudicial to the security of the premises and the material and equipment mentioned in Regulation 4(2).

108. Although comprehensive and partially effective in managing undue burden, such an approach takes no account of the actual security risk that results from work being carried out. Inspectors should note that in line with the implementation of outcome focussed regulation, there is an opportunity to manage the requirement for a TSP based on the risk associated with whatever is planned and the consequent impact on nuclear security if inadequately conceived or executed. This can be done by reissuing a risk based, rather than prescriptive Regulation 8(2) notification.

109. The key consideration is that the dutyholder has a robust and consistent methodology that enables the level of risk involved to be identified and work graded accordingly. That methodology must be included or specifically referenced in the extant security plan and ONR approval will include issuing a Regulation 8(2) notification reflecting the arrangements. ONR has an expectation that the process has appropriate internal assurance oversight, and all works are recorded to enable sampling as necessary. Some smaller sites, or those in steady state, may not wish to develop these arrangements. In these cases, ONR will continue to issue a prescriptive Regulation 8(2) notification.

110. Regulation 8(3) reiterates that applications for TSPs must be made in writing. Inspectors should be aware that ONR expects to receive applications at least 28 days before work is due to commence to allow adequate time to assess and formally approve a proposal. Regulation 8(4) requires a responsible person to maintain an adequate level of security while work is taking place and describe how this will be achieved in the TSP. It is in their interest to make the TSP as clear as possible and ONR expects to see accompanying drawings, photographs, explanatory notes to help understand the work taking place and resultant security risk.

111. A TSP should also specify the start and finish dates. Where work is likely to last for more than 12 months an amendment to the extant approved security plan should be considered instead of a TSP. The responsible person must also consider if on completion of a TSP the work will necessitate an amendment to the security plan. ONR will review any TSP that, for whatever reason, is not closed within 12 months. Inspectors should confirm that all TSPs have been developed using the dutyholder's processes for changes to SPA to determine the impact of the proposed change on the extant PPS and delivery of relevant outcomes described in the security plan.

112. Inspectors should expect to see sign-off by internal assurance (or equivalent) and the CNC Operational Unit Commander / Civilian Guard Force manager where officers / guards will be required to support the revised security arrangements as part of the change management process. Arrangements for producing TSP and seeking ONR approval (as necessary), must be described in the extant approved security plan or explicitly referenced within it. ONR may

require amendment of a temporary security plan prior to its approval under Regulation 8(5).

113. Regulation 8(6) and (7) remind responsible persons to comply with the extant approved site security plan in addition to the arrangements covered in a temporary security plan. ONR can inspect any aspect of a responsible person's security arrangements at any time to confirm they comply with those stated in the plan(s). Inspectors should note that once a TSP is approved it becomes an integral part of the wider security plan.

114. Regulation 8(8) enables a responsible person to amend an approved TSP. The process for approving any change is as stated above.

115. Further guidance on the need for and management of temporary security plans and Regulation 8(2) notifications can be found in the managing changes to SPA TAG.

116. A Regulation 8(2) notification is available for use at Appendix 14.

7.6. Regulation 9 – Requirement for Approval of Relevant Personnel

The responsible person in relation to each nuclear premises must ensure that each of his relevant personnel in relation to the premises who—

(a) is specified in the approved security plan for the premises as requiring investigation and assessment as mentioned in regulation 4(3)(a), or

(b) falls within a description of persons who are so specified,

is a person who has been assessed, in accordance with a process that has been approved by the ONR, to be of suitable character and integrity, having regard to the need to ensure the security of the premises and the material, equipment and information mentioned in regulation 4(2).

117. Inspectors should be aware that NISR 2003 requires the responsible person to ensure that its personnel (and those of its contractors) with access to the nuclear premises or to nuclear material/ORM2, SNI and/or equipment / software used or stored on the premises in connection with activities involving nuclear material / ORM, are assessed in accordance with a process that has been approved by the ONR, to be of suitable character and integrity. For this purpose, the HM Government Baseline Personnel Security Standard (BPSS), which is a pre-employment control, and National Security Vetting (NSV) have been established as the approved process. Three levels of NSV clearances exist: Developed Vetting (DV); Security Check (SC) and Counter Terrorist

[2] Cat IV NM and ORM only where the premises is also a nuclear site.

Check (CTC). ONR is the Vetting Authority for the regulated civil nuclear industry.

118. HMG has published standards that are to be achieved in relation to the BPSS and NSV. This is publicised by way of the 'HMG Baseline Personnel Security Standard – Guidance on the Pre-employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors' and, the 'OFFICIAL-SENSITIVE HMG Personnel Security Supplement to the Security Policy Framework. Additional ONR requirements (e.g., relating to overseas police certificates, restrictions on what dutyholders may approve, etc.) are identified in the ONR Workforce Trustworthiness Technical Assessment Guides and Annex L of the O-S: SNI Annexes to the SyAPs [2].

119. Regulation 4(3)(a) requires that inspectors should confirm that security plans include details of the personnel security SPA applied by the responsible person to meet ONR expectations that facilitate ONR's investigation and assessment of the suitability of personnel with access to their premises, Nuclear Material/ORM, software, equipment and information described in Regulation 4(2). This will include ensuring the security plan meets the clearance levels mandated within Annex K of the O-S: SNI Annexes to SyAPs.

120. ONR, as a Vetting Authority, approves individuals working within the civil nuclear sector for national security vetting. ONR also approves a dutyholder's processes and compliance with mandated clearance requirements specified or referenced within the security plan. NISR 2003 was amended in 2017 to reflect that dutyholders, rather than ONR, complete the Baseline Personnel Security Standard process (a pre-employment control) where it falls within their signing authorities. Similar amendments have been made to Regulation 17(3) and 22(7).

121. An ongoing assurance of character and integrity is obtained through HMG mandated ongoing personnel security reporting arrangements for NSV holders. At DV, an Annual Security Appraisal Form (ASAF) is required, and a Change of Personal Circumstances Questionnaire must be completed by individuals where there is a change of name or living arrangements; criminality (including arrest); nationality; and at SC/DV, finances. Assurance that these arrangements exist are to be referenced in the security plan.

122. An effective ongoing personnel security culture, ensuring that sponsors are aware of aftercare incidents that must be reported for NSV holders to ONR as the Vetting Authority, or at BPSS that are to be managed locally, can only be effective if there is a joined-up approach between Security, Human Resources, Occupational Health and Line Managers. This includes those departments within the supply chain. Inspectors will wish to ensure that requirements identified in Co-Operation of Departments with Responsibility for Delivering Vetting and Ongoing Personnel Security Arrangements are reflected in the security plan [9]. This will include having relevant policies on such issues as Reporting Hotlines, social media, Harassment and Bullying, Employee Assistance Programmes which have the potential to mitigate the

insider threat and which in some instances are policies mandated in the HMG Personnel Security Supplement to the SPF.

7.7. Regulation 10 – Reports by Responsible Persons

(1) The responsible person in relation to each nuclear premises must report to the ONR any event or matter of a kind specified in paragraph (5) as soon as practicable and in any event within 24 hours of its becoming known to him.

(2) If it is not possible for him to make a written report within that period, he must make the report orally and confirm it in writing within 48 hours of the event or matter becoming known to him.

(3) In any other case the report must be made in writing.

(4) The report must specify the nature of the matter or event and, in the case of an event, the date and time it occurred and the apparent reason for it.

(5) The events and matters are—

(a) any unauthorised incursion on to the premises or any attempted or suspected such incursion;

(b) any incident occurring on the premises involving an explosive or incendiary device or suspected such device, or a firearm or replica firearm;

(c) any damage to any building or equipment on the premises which might affect the security of the premises or any material or equipment mentioned in regulation 4(2); (d) any malicious damage to any building or equipment on the premises, other than any trivial damage that does not affect the security of the premises or any material or equipment mentioned in regulation 4(2);

(e) any theft or attempted theft, or any loss or suspected loss, or any unauthorised movement—

(i) of any nuclear material used or stored on the premises or in transit to or from them, or

(ii) in the case of premises which are or form part of a nuclear site, of any other radioactive material used or stored on them;

(f) any theft or attempted theft, or any loss or unauthorised disclosure, of sensitive nuclear information kept on the premises, or any suspected such theft, loss or disclosure;

(g) any unauthorised access to any sensitive nuclear information kept on the premises, or any attempt to gain such access;

(h) any threat to do anything which would fall within any of sub-paragraphs (a) to (g);

(i) any failure to comply with any of the standards, procedures and arrangements described in the approved security plan for the premises or in any approved temporary security plan to which for the time being they are subject;

(j) any other event or matter which might affect the security of the premises or the material, equipment or information mentioned in regulation 4(2).

123. NISR 2003 requires a responsible person to report the events prescribed in Regulation 10(5) to ONR. Inspectors should be aware that reports must be made "as soon as practicable" and in any event within 24 hours of the event occurring. An event might be part of concerted activity against civil nuclear sites that could, for example, necessitate a change to the CT response level. Prompt reporting enables timely assessment and threat mitigation.

124. To enable expedient reporting, initial reports may be made orally, with written confirmation sent by means of an INF1 form [10] within 48 hours of the event. Failure to report a prescribed event is an offence under NISR 2003; inspectors should remind the dutyholder that they should not delay reporting because they do not have all the facts, are conducting their own investigation, or are awaiting confirmation as to whether a suspected event or matter actually occurred.

125. During working hours, reports should normally be made to the nominated site security inspector. Where reasonable attempts have been made by the dutyholder to communicate the report via this method are unsuccessful, then the out-of-hours system may be utilised. This is through the CNSS Duty Officer, via the CNC communications centre (this number can be found on the INF 1 form).

126. The onus is on the responsible person to ensure ONR receives event reports. Sending an email to, or leaving a voicemail for the site inspector, does not constitute a Regulation 10 report until receipt is confirmed (i.e., telephone or email reply (not an Out of Office message)). If a report is made via the CNC communications centre, the responsible person should still confirm ONR has received it. Reports to the CNC communications centre, or any other third party, do not discharge their responsibilities under Regulation 10.

127. Events and matters covered under Regulation 10(5) (a) – (h) must be reported regardless of their effect on security. Those falling under Regulation 10(5) (i) may not have to be reported where a Regulation 7(2) notification has been issued stating that the event or matter is of a kind unlikely to be prejudicial to

security or be of any press interest and therefore does not need to be submitted to ONR.

128. Regulation 10 (5) (j) is designed to ensure an event that does not fall under any other category is still reported. Similar to Regulation 10(5) (i), the Regulation 7(2) notification can be used to determine events or matters of a kind unlikely to be prejudicial to security or be of any press interest and therefore do not need to be submitted to ONR.

129. In either case, dutyholders should take a conservative approach to reporting. This means that where the dutyholder is in any doubt about whether any particular Regulation 10 (i) or (j) event or matter meets the reporting threshold then the default position should be to contact ONR to confirm the requirement. Dutyholders may also contact ONR for advice on the correct categorisation of events and the initial determination of significance.

130. All events or matters, regardless of the need to submit to ONR, should be recorded and made available for operational experience and trending analysis.

Table 3 – Guidance on NISR 2003 Regulation 10 Reporting

ONR Category	Description
Major	Incursions or other malicious activity conducted against the site; or, where all key control measures necessary to satisfy the delivery of security outcomes and relevant good practices have been, or are likely to be, compromised, which could result in a serious consequence.
Moderate	Where one or more key control measures necessary to satisfy the security outcomes or relevant good practice have been, or likely to be, significantly weakened, which could result in a significant consequence.
Minor	Where the key control measures necessary to satisfy security outcomes and relevant outcomes remain broadly effective but could result in a minor consequence.
None	Where there has been an event or matter that has no security affect or consequence.

Regulation	Description
10 (5) (a-h)	*(a) Any unauthorised incursion on to the premises or any attempted or suspected such incursion.* *(b) Any incident occurring on the premises involving an explosive or incendiary device or suspected such device, or a firearm or replica firearm.* *(c) Any damage to any building or equipment on the premises which might affect the security of the premises or any material or equipment mentioned in regulation 4(2).* *(d) any malicious damage to any building or equipment on the premises, other than any trivial damage that does not affect the security of the premises or any material or equipment mentioned in regulation 4(2);* *(e) any theft or attempted theft, or any loss or suspected loss, or any unauthorised movement—* *(i) of any nuclear material used or stored on the premises or in transit to or from them, or* *(ii) in the case of premises which are or form part of a nuclear site, of any other radioactive material used or stored on them;* *(f) any theft or attempted theft, or any loss or unauthorised disclosure, of sensitive nuclear information kept on the premises, or any suspected such theft, loss or disclosure;* *(g) any unauthorised access to any sensitive nuclear information kept on the premises, or any attempt to gain such access;* *(h) any threat to do anything which would fall within any of sub-paragraphs (a) to (g);*

Regulation	Description
	1. Typical **Major** examples might include: a. Confirmed site incursion. b. Any act or attempted act of sabotage to security assets on a site, including cyber attack c. Any act or attempted act of sabotage on nuclear material/ORM or associated buildings and facilities d. Any loss, theft or attempted theft of Cat I-III Nuclear Material / Group A/B Other Radioactive Material or information security classified as SECRET e. Confirmed compromise of information classified as SECRET or above (e.g., highly detailed and exploitable information regarding Category I-III nuclear material or vital areas that may jeopardise an effective nuclear security response; or that which could seriously damage international relations) f. Confirmed compromise of operational technology categorised as 'Critical' or 'Major' impact. g. Confirmed compromise of IT and/or associated network(s) handling information security classified as SECRET or above. 2. Typical **Moderate** events might include: a. Attempted or suspected incursion. b. Damage to any building or equipment which might affect the security of the premises or nuclear material/ORM held thereon. c. Any loss, theft or attempted theft of Category IV nuclear material or Group C/D ORM. d. Confirmed compromise of information classified as OFFICIAL-SENSITIVE:SNI (e.g., information likely to be of minimal consequence to nuclear security if compromised; or that which could have other damaging consequences if lost, stolen or published in the media) e. Confirmed compromise of operational technology categorised as 'Significant' or 'Minor' impact. f. Confirmed compromise of IT and/or associated network(s) handling information security classified as OFFICIAL-SENSITIVE:SNI 3. Typical **Minor** events might include: a. Failed attempt to gain unauthorised access. b. Actual or Attempted act to cause malicious damage to asset not associated with site security or nuclear material/ORM. c. Significant anomalous activity or other indicator of compromise to equipment or software used in connection with activities involving nuclear material/ORM requiring further investigation (confirmation of compromise would necessitate an uplift of event grading).

Regulation	Description
	d. Significant anomalous activity or indicator of compromise identified on IT and associated networks handling SNI that requires further investigation (confirmation of compromise would necessitate an uplift of event grading). e. A reasonable suspicion of the loss or compromise of OFFICIAL-SENSITIVE:SNI or information that is reportable in accordance with the Collaboration on Gas Centrifuge Technology Handbook on Security of Classified Information, that requires further investigation (confirmation of compromise would necessitate an uplift in the event grading).
10 (5) (i)	*Any failure to comply with any of the standards, procedures and arrangements described in the approved security plan for the premises or in any approved temporary security plan to which for the time being they are subject.* 4. Typical **Major** events might include: a. Pass and PIN handed to another individual in order to gain access to protected or inner area for malicious purposes. b. Total loss of security management system. c. 5. Typical **Moderate** events might include: a. Visitors left unescorted/insufficiently supervised in a protected or inner area. b. Security boundary door found unsecured, and alarm inhibited but with other layers of defence in depth in place and effective. c. Breaches of procedure in the arrangements to protect information security classified as SECRET or above where there is no suspicion of loss or compromise. d. Non-compliance with search regime at entry points to a protected or inner area. e. Pass and PIN handed to another individual in order to gain access to restricted area. f. Site pass issued for protected or inner area without correct clearance in place. g. No CNC Operational Firearms Commander. h. Security staff or CNC shortfall that significantly affects the security response. i. Significant proportion of Security Management System lost. 6. Typical **Minor** events might include: a. Visitors left unescorted/insufficiently supervised in a limited access area. b. Temporary loss of small section of PIDS or IDS coverage.

Regulation	Description
	c. Breaches of procedure in the arrangements to protect information security classified as OFFICIAL-SENSITIVE:SNI where there is no suspicion of loss or compromise d. Non-compliance with search regime at entry points to a limited access area. e. Security boundary door found locked, but alarm inhibited with other layers of defence in depth in place and effective. f. Site pass issued for limited access area without necessary clearance or clearance having expired. g. Employee allowed site access on expired pass. h. Security staffing shortfall (including CNC) which affects security regime. i. Authorised member of staff given access to site on expired pass. j. Lost site pass not reported correctly.
10 (5)(j)	*Any other event or matter which might affect the security of premises or the material, equipment or information mentioned in regulation 4(2).* 7. Typical **Moderate** Events might include: a. Discovery of prohibited (unless covered by 10(b) above) items onsite. b. Large, organised protest or gathering in proximity to the site. 8. Typical **Minor** events might include: a. Attempt to bring prohibited (unless covered by 10(b) above) item onto site. b. Discovery of lost or mislaid pass on-site. c. Alarm activated, investigated and found to be spurious. d. Member of public filming or acting suspiciously in proximity to site. e. Acts of criminality on site indicating staff behaviours of concern regarding honesty and integrity.

7.8. Regulation 11 – Directions to Responsible Persons

(1) The responsible person in relation to each nuclear premises must comply with any direction given by the ONR for the nuclear security purposes (within the meaning of section 70 of the Energy Act 2013) requiring him—

(a) to adopt or implement, in respect of the whole or any specified part of the premises, standards, procedures or arrangements specified in the direction and to secure that the responsible person's officers, employees, contractors and consultants comply with them,

(b) to submit a fresh security plan or amendments of the approved security plan for the premises to the ONR for approval,

(c) to satisfy the ONR about the continuing or future adequacy of the approved security plan for the premises, or that the responsible person is complying with it,

(d) to record or investigate in such manner as is specified in the direction—

(i) any event or matter of a kind specified in regulation 10(5), or

(ii) any such other event or matter as is specified in the direction, or to report, in such manner as is specified in the direction, to the ONR , or such other person as is so specified, any such other event or matter as is so specified, or

(e) to take such steps as the ONR considers necessary to remedy or alleviate the consequences of any contravention of these Regulations.

(2) Such a direction may impose a requirement to be met—

(a) within a period specified in the direction, or

(b) in the case of a direction under paragraph (1)(c), periodically at such intervals as are specified in the direction.

(3) Any direction given by the ONR to a person on or after 1st April 2014 under paragraph (1)—

(a) is subject to any 2001 Act direction given to the person whenever given; and

(b) must state that it is subject to any such 2001 Act direction.

131. Inspectors should be aware that NISR 2003 Regulation 11(1) specifically relates to nuclear premises and the requirement for responsible person to

comply with any direction given by ONR in respect of security standards, procedures and arrangements. Directions might require responsible persons to:

1) Modify a specified aspect of the extant security arrangements and ensure the change is complied with - e.g., vulnerability has been identified during inspection which requires addressing. Whilst ONR would seek to influence improvements, dutyholder inaction or attitude may require a more formal enforcement action to ensure appropriate resolution. ONR inspectors should refer to the ONR Enforcement Management Model (EMM) for further guidance [11].

2) Submit a new security plan for approval; - This might be required in response to ONR's concerns regarding the currency of the plan as a consequence of changes to the DBT or site operations that invalidate the basis of the security plan.

3) Confirm the extant plan is fit for purpose and they are compliant with it – ONR's expectation detailed in SyAPs is that security plans will be subject to periodic reviews. This is important to ensure that small iterative changes are considered as a collective whole and that the dutyholder takes into account changes in relevant good practice. It should be noted that such a review may require amendments to be submitted in accordance with Regulation 6.

4) To:

    i. Record or investigate an event covered by Regulation 10(5) or as specified in the direction;

    ii. Provide a report in accordance with the direction;

    iii. Take whatever steps ONR considers necessary to correct or mitigate any non-compliance with the extant plan. This is extremely broad and powerful and should always be subject to the principles of the Regulators Code.

132. Unlike an improvement or prohibition notice issued under the HSWA 1974, inspectors should note that dutyholders have no recourse of appeal to a tribunal against a direction. Dutyholders nevertheless do have the right to judicial review. However, it should be noted that similar to a prohibition notice, security directions have legal effect from the time of issue rather than being placed on hold pending the outcome of any review.

133. A judicial review is where a High Court Judge sitting in the Administrative Court considers whether an action or decision of a public authority is lawful. They are normally looking at either:

    i. whether a public authority has properly followed the policies it has in place; or sometimes, more broadly,

ii. whether the policy itself is unlawful in some way.

134. The procedure initially involves a Claimant (or their legal representative) sending a pre-action letter, which gives the public authority a chance to resolve the cases where a mistake may have been made by the person making the decision. But if the public authority stands by its policy/decision, proceedings may be started, and the court will decide whether it is unlawful. Generally, where the court finds in favour of the Claimant, the remedy is an instruction to the public authority to retake the decision properly/fairly, or to reconsider the policy it has in place and replace it with a different one which is not unlawful. The court normally does not substitute the public authority's decision with its own decision (or policy), so in that respect it is different to an appeal to a Tribunal where a new decision is often simply imposed.

135. Regulation 11(2) enables ONR to place a time limit on meeting a direction or, where confirmation of continuing compliance is required, the periodicity of progress reports. Examples could include monitoring progress security improvement schedule projects or other major changes. However, ONR's regulatory approach is for influencing and enabling to be exhausted before formal enforcement action is taken.

136. Template directions are available through HOW2 under 'Enforcement' and into the 'Legal Forms' box.

8. NISR Part 3 - Security of Transport of Nuclear Material

8.1. Regulation 13 – Requirement for Category I/II Nuclear Material and Category III Nuclear Material to be Transported by Approved Carriers

(1) No person shall transport any Category I/II nuclear material unless—

(a)he is a carrier who is for the time being approved by the ONR as a Class A carrier to transport Category I/II nuclear material and Category III nuclear material, or

(b)he is doing so as an officer or employee of such a carrier.

(2) No person shall transport any Category III nuclear material unless—

(a) he is a carrier who is for the time being approved by the ONR as a Class A carrier to transport Category I/II nuclear material and Category III nuclear material,

(b) he is a carrier who is for the time being approved by the ONR as a Class B carrier to transport Category III nuclear material, or

(c) he is doing so as an officer or employee of a carrier falling within sub-paragraphs (a) or (b).

(3) If the responsible person in relation to any nuclear premises arranges for the transport of any Category I/II nuclear material or Category III nuclear material to or from the premises, he must ensure that the transport is undertaken by a carrier who is not prohibited under this regulation from transporting the material in question.

137. Regulation 3 provides detailed information on the categorisation of nuclear material and inspectors should use it in conjunction with this section of the guidance document. Inspectors should note that whilst non-nuclear materials meeting the irradiated criteria (refer to paragraph A1.40) are considered Category III for physical protection purposes whilst on nuclear sites[3] (licensed) they are considered to be Category IV for transport purposes and are not covered by NISR 2003 when in transit. Instead, aspects of security by road and rail in Great Britain are regulated by ONR under CDG 7 / ADR /RID. Road Travel in Northern Ireland is regulated separately. Air and sea transport is regulated by the Civil Aviation Authority and Coastguard Agency respectively under their own legislation.

[3] When categorised against SyAPs Annex A, Table 1

138. If the dutyholder (see Regulation 2(2)) in relation to any nuclear premises arranges for transport of Category I/II or III material to or from the premises, they must ensure that the transport is undertaken by an approved carrier.

8.2. Regulation 14 – Approval of Carriers

(1) The ONR may approve a carrier as an approved carrier only if she is satisfied that—

(a)in the case of an approval as a Class A carrier, the carrier transports or proposes to transport Category I/II nuclear material in the course of his business,

(b)in the case of an approval as a Class B carrier, the carrier transports or proposes to transport Category III nuclear material in the course of his business,

(c)the carrier has provided the ONR with—

(i) his telephone number, facsimile number and principal place of business,

(ii) the name, address, telephone number and facsimile number of an individual who will accept any written or oral communication from the ONR under these Regulations on behalf of the carrier, and

(d)the carrier has submitted a transport security statement under Regulation 16 that the ONR has approved (as submitted or with such amendments as she has required), and he will comply with the standards, procedures and arrangements described in the approved transport security statement while he is approved.

139. Inspectors should be aware that the approval process for a TSS is likely to take a minimum of 2 months for a Class B approved carrier, and longer for a Class A approved carrier. ONR encourages carriers to contact ONR, in advance of the application as soon as it becomes apparent that they may be asked to transport nuclear material as described in the Schedule to NISR 2003.

140. Applicants wishing to become a Class A or Class B approved carrier will need to demonstrate how the relevant security outcomes in SyAPs would be achieved. Prescriptive guidance (Guidance for Class B Carriers (GCBC)) is available to assist those wishing to become Class B approved carriers in view of the lower hazard and risk associated with this material and in recognition of the likely security resource such carriers have. Inspectors should be aware that this guidance is security classified OS:SNI and is available on request provided need-to-know criteria are met.

141. Inspectors should expect applications to contain the following information on the applicant, their business and security procedures:

a) where the applicant is a body required by law to be Registered by the Registrar of companies, the name, Registered number and Registered office of that body;

b) where the applicant is an association or partnership which is not required by law to be so Registered, the full name of each member of the association or each partner in the partnership, and the name of the association or partnership, as the case may be;

c) where the applicant is a sole proprietor, the full name of that proprietor;

d) the applicant's trading name, if different from the name given above;

e) the telephone number, fax number if any, and address of the principal office and of all premises from where nuclear material is handled by the applicant;

f) the name, telephone number, fax number if any, and address within the United Kingdom of an individual who will act as the main contact point including for the receipt of any document mentioned in the Regulations from the ONR relating to nuclear material carriage;

g) any changes to the applicant's trading activities in the past five years must be given;

h) the number of staff engaged by the applicant in the handling and carriage of nuclear material;

i) the mode or modes of transport for which the applicant is seeking approval, i.e., road, rail and / or sea;

j) the Category or Categories of nuclear material to be carried; and

k) a "Transport Security Statement" describing the security standards, procedures and arrangements in place for the protection of nuclear material and sensitive nuclear information, including appropriate security clearance procedures for those personnel concerned, and arrangements during any temporary cessation of such transport, i.e., during any planned stops enroute. The carrier will submit the plan in accordance with Regulation 16.

(2) Where a carrier has applied to the ONR for approval as an approved carrier, the ONR must give him notice in writing of the ONR decision and, if the ONR has granted the application, of the date from which he is approved and whether he is approved as a Class A carrier or as a Class B carrier.

(3) If the ONR proposes not to approve a carrier as an approved carrier, the ONR must give him written notice of the ONR proposal and of the reasons for it.

(4) The carrier may make representations to the ONR within 28 days from the date on which the notice under paragraph (3) is given.

(5) The ONR must take into account any such representations before reaching a decision whether to approve the carrier as an approved carrier.

(6) If the ONR decides not to approve a carrier as an approved carrier, the ONR must state the reasons for the ONR decision when the ONR gives him notice of the decision under paragraph (2).

142. The remainder of these regulations explain the actions ONR must take and are considered self-explanatory. Inspectors should seek to keep prospective carriers informed on the progress of their application through an enabling regulation approach.

(7) The ONR 's approval of a carrier as an approved carrier has effect for the period of five years from the date from which he is approved, unless it is revoked earlier under Regulation 15.

143. Inspectors should be aware that this regulation simply confirms that approved carrier status last for 5 years unless it is revoked earlier.

8.3. Regulation 15 – Revocation of Approved Carriers

(1) The ONR may revoke the approval of an approved carrier if he has requested that his approval be revoked or on any of the following grounds—

(a) that—

(i) in the case of a Class A carrier, he has ceased to carry on a business as a carrier of Category I/II nuclear material, or

(ii) in the case of a Class B carrier, he has ceased to carry on a business as a carrier of Category III nuclear material;

(b) that he has failed to comply with any obligation imposed on him under these Regulations;

(c) that he has supplied false or misleading information in his application for approval as an approved carrier or has failed to supply information that was material to the application; or

(d) that the ONR is of the view that the approval should be revoked in the interests of ensuring the security of the Category I/II nuclear material

or Category III nuclear material that the approved carrier might otherwise transport.

(2) If the ONR proposes to revoke the approval of an approved carrier otherwise than pursuant to a request from him, the ONR must give him written notice of the ONR proposal and of the reasons for it.

(3) The approved carrier may make representations to the ONR within 28 days from the date on which the notice under paragraph (2) is given.

(4) The ONR must take into account any such representations before reaching a decision whether to revoke the approved carrier's approval.

(5) If the ONR decides to revoke the approval of an approved carrier, the ONR must give him written notice of the ONR decision and of the reasons for it.

144. If ONR intends cancelling the approval of an approved carrier, other than following a request from the carrier, ONR must provide written notice of the proposal and the reasons for it. The approved carrier may appeal to ONR within 28 days from the date of the notice.

Appeals

145. Inspectors should be aware that ONR must take into account any such appeal in accordance with ONR's Decision Review and Appeals Process [12] before reaching a decision whether to revoke the approved status of the carrier.

146. Any failure by an approved carrier to comply with any obligation will be subject to appropriate consideration utilising the EMM. A unilateral decision by ONR to revoke an approved carrier's approval on the grounds outlined in sub-paragraphs b - d is a significant step and may attract external scrutiny. That should not constrain an inspector in making their judgement, but should be borne in mind when preparing documents, exchanging e-mails etc.

8.4. Regulation 16 – Transport Security Statements

(1) A carrier applying for approval as a Class A carrier or Class B carrier under regulation 14 must submit with his application a transport security statement for approval by the ONR.

(2) The transport security statement must describe in writing the standards, procedures and arrangements adopted or to be adopted by the carrier to ensure the security of—

(a) in the case of a carrier applying for approval as a Class A carrier, any Category I/II nuclear material or Category III nuclear material transported or to be transported by him,

(b) in the case of a carrier applying for approval as a Class B carrier, any Category III nuclear material transported or to be transported by him, and

(c) in any case, any information which is or comes within his possession or control relating to the security of any nuclear premises or of any Category I/II nuclear material or Category III nuclear material transported or to be transported by him.

(3) In particular, but without prejudice to the generality of paragraph (2), the statement must describe the standards, procedures and arrangements relating to—

(a) the investigation and assessment by the ONR of the suitability of relevant personnel of the carrier with a view to ensuring the security of—

(i) any Category I/II nuclear material or Category III nuclear material transported or to be transported by the carrier,

(ii) any information falling within paragraph (2)(c), and

(iii) any nuclear premises to or from which the carrier transports or is to transport any Category I/II nuclear material or Category III nuclear material, and any premises used or to be used for the purpose of the temporary storage of such material during the course of or incidental to its transport,

(b) the temporary storage of Category I/II nuclear material or Category III nuclear material during the course of or incidental to its transport, including the security of premises used for such storage, and

(c) the steps to be taken by the carrier or any person acting on his behalf if any event of a kind specified in regulation 18(5)(a), (b), (c), (f), (g), (h) or (i) that requires immediate action occurs, and the regular practice of the activities required in connection with those steps.

(4) The ONR may approve the statement as submitted or with such amendments as the ONR may require.

(5) An approved carrier may at any time submit to the ONR for approval—

(a) a fresh transport security statement, or

(b) proposals for amending his approved transport security statement.

(6) The ONR may approve the fresh statement or proposals as submitted or with such amendments as the ONR may require.

(7) On approving a fresh transport security statement for an approved carrier, the ONR may revoke the approval of the former statement for the approved carrier.

147. Inspectors should be aware that the TSS must describe in writing the SPA adopted or to be adopted by the carrier to ensure the security of material transported by them and what they can legally transport (i.e., Category III nuclear material in the case of a Class B carrier). The TSS will be assessed for adequacy using SyAPs and/or the GCBC together with appropriate TAGs.

148. The TSS must also describe the carrier's SPA for the personnel security of relevant employees and contractors to mitigate the risk of insider threats to nuclear material being transported and any associated SNI. Thus, inspectors should bear in mind the national security vetting status and levels of the approved carrier's personnel (staff and contractors) involved in the movement of nuclear material and/or with access to SNI.

149. A TSS should describe the SPA for the temporary storage of Category I/II nuclear material or Category III nuclear material during the course of, or incidental to, its transport, including the security of premises where material is stored.

150. The TSS must cover responsibility and the arrangements for reporting if any event specified in Regulation 18(5) (a), (b), (c), (f) or (i) that requires immediate action occurs and an approved carrier should have a range of contingency plans to deal with a range of events from a puncture to a terrorist attack. Regular practicing or exercising contingency plans will provide inspectors with assurance on their effectiveness.

151. Through a combination of early engagement by a prospective carrier and an enabling approach by inspectors, ONR hopes to approve a TSS on first submission. If amendment is needed inspectors should continue with an enabling approach to assist carriers achieve approval.

152. Inspectors should be aware that carriers may submit a new TSS or amendments to an existing plan for approval at any time. Following approval of the new plan, ONR will revoke the existing plan.

8.5. Regulation 17 – Duties of Approved Carriers: General

(1) An approved carrier must comply with the standards, procedures and arrangements described in his approved transport security statement.

(2) An approved carrier must notify the ONR of any change to the information referred to in regulation 14(1)(c)—

(a) in the case of information referred to in regulation 14(1)(c)(i), within 7 days of the change occurring, and

(b) in the case of information referred to in regulation 14(1)(c)(ii), no later than the change occurs.

(3) An approved carrier must ensure that each of his relevant personnel who—

(a) is specified in his approved transport security statement as requiring investigation and assessment as mentioned in regulation 16(3)(a), or

(b) falls within a description of persons who are so specified

*is a person who has been **[** assessed, in accordance with a process that has been approved by the ONR, to be **] 2** of suitable character and integrity, having regard to the need to ensure the security of the material, information and premises mentioned in regulation 16(3)(a).*

153. Inspectors should be aware this regulation requires that the approved TSS is current and reflects the SPA a carrier must follow, including the personnel security of staff and contractors. The changes in this regulation cover administrative changes such as contact details and nominated point of contact. Unlike a site security plan there is no provision for a temporary change to a TSS.

8.6. Regulation 18 – Reports by Carriers

*(1) An approved carrier must report to the **[**ONR**] 1** any event or matter of a kind specified in paragraph (5) as soon as practicable and in any event within 24 hours of its becoming known to him.*

*(2) If it is not **[** possible **] 2** for him to make a written report within that period, he must make the report orally and confirm it in writing within 48 hours of the event or matter becoming known to him.*

(3) In any other case the report must be made in writing.

(4) The report must specify the nature of the matter or event and, in the case of an event, the date and time it occurred and the apparent reason for it.

(5) The events and matters are—

(a) any unauthorised incursion on to, interference with, or other incident affecting the security of any means of conveyance of Category I/II nuclear material or Category III nuclear material during the course of its transport or any attempted or suspected such incursion, interference or incident;

(b) any unauthorised incursion on to premises where Category I/II nuclear material or Category III nuclear material is being stored temporarily during the course of or incidental to its transport or any attempted or suspected such incursion;

(c) any incident occurring during the transport of Category I/II nuclear material or Category III nuclear material, or on premises where such material is being stored temporarily during the course of or incidental to its transport, involving an explosive or incendiary device or suspected such device, or a firearm or replica firearm;

(d) any damage to the means of conveyance of Category I/II nuclear material or Category III nuclear material which might affect the security of that material;

(e) any damage to any building or equipment on premises where Category I/II nuclear material or Category III nuclear material is being stored temporarily during the course of or incidental to its transport which might affect the security of the material;

(f) any theft or attempted theft, or any loss or suspected loss, or any unauthorised movement of, or any interference with, Category I/II nuclear material or Category III nuclear material during transport;

(g) any theft or attempted theft, or any loss or unauthorised disclosure, of information falling within regulation 16(2)(c), or any suspected such theft, loss or disclosure;

(h) any unauthorised access to any such information or any attempt to gain such access;

(i) any threat to do anything which would fall within any of sub-paragraphs (a) to (h);

(j) any failure to comply with any of the standards, procedures and arrangements described in the approved carrier's approved transport security statement or the measures described in any approved transport plan required under regulation 19;

(k) any other event or matter which might affect the security of—

(i) Category I/II nuclear material or Category III nuclear material being transported,

(ii) premises where Category I/II nuclear material or Category III nuclear material is being stored temporarily during the course of or incidental to its transport, or (iii) any information falling within regulation 16(2)(c).

154. Inspectors should be aware that NISR 2003 requires carriers to notify ONR should an event occur that is prescribed in Regulation 18(5). Reports must be made “as soon as practicable” and in any event within 24 hours of the event occurring. An event might be part of concerted activity against civil nuclear sites that could, for example, necessitate a change to the CT response level. Prompt reporting enables timely assessment and threat mitigation.

155. To enable expedient reporting, initial reports may be made orally, with written confirmation sent by means of an INF1 form within 48 hours of the event. Failure to report a prescribed event is an offence under NISR 2003; inspectors should remind the dutyholder that they should not delay reporting because they do not have all the facts, are conducting their own investigation, or are awaiting confirmation as to whether a suspected event or matter actually occurred.

156. The report must specify the nature of the matter or event and in the case of an event, the date and time it occurred and the apparent reason for the occurrence.

157. During working hours, reports will normally be made to the nominated transport security inspector. It this is not possible, or an event occurs out-of-hours, a report should be made to the CNSS Duty Officer either direct or via the CNC communications centre (this number can be found on the INF1 form).

158. Inspectors should be aware that the onus is on the responsible person to ensure ONR receives event reports. Sending an email to, or leaving a voicemail for the transport inspector, does not constitute a Regulation 18 report until receipt is confirmed (i.e., telephone or email reply (not an Out of Office message)). If a report is made via the CNC communications centre, the responsible person should still confirm ONR has received it. Reports to the CNC communications centre, or any other third party, do not discharge the legal duty under Regulation 18.

159. Transport Security is an ONR CNSS specialism. Inspectors should, therefore, be aware of and familiarise themselves with the relevant guidance; including the ONR – Nuclear Transport Security – GCBC. If a CNSS Duty Officer receives a report under Regulation 18 out-of-hours, additional advice may be available from the Transport Inspectors.

160. The most likely type of event an approved carrier would report to ONR of is a mechanical breakdown during a Category III movement. Inspectors should note that it is the carrier's responsibility to ensure continued protection of the load and recovery through application of their contingency plans (not the CNC or Home Department Police Force/Police Scotland Police).

161. During the movement of Category I/II nuclear material the Transport Security Inspectors will ensure the ONR CNS Duty Officer / Director are informed that a move is taking place; a Transport Inspector will usually be available for advice. The CNC will instigate full Command and Control (C2) arrangements to coordinate the protection of the transport at all times.

162. All events and matters covered under Regulation 18(5) (a) – (j) must be reported. Regulation 18(5) (k) is designed to ensure an event that does not fall under any other category is still reported. Whilst NISR does not allow the issue of notifications to define a threshold below which a non-compliance with the Transport Security Statement (TSS or Transport Security Plan (TptSP) need not be reported (as is the case for nuclear premises), carriers may

develop, and agree with ONR, their own framework to determine the types of event or matter that will and will not be submitted to ONR under Regulation 18(5) (k).

163. In either case, carriers should take a conservative approach to reporting. This means that where the carrier is in any doubt about whether a particular event or matter meets the reporting threshold then the default position should be to contact ONR to confirm the requirement. Dutyholders may also contact ONR for advice on the correct categorisation of events and the initial determination of significance.

164. All events or matters, regardless of the need to submit to ONR, should be recorded and effectively managed (e.g., assessed, mitigated and follow-up action taken to prevent reoccurrence, as appropriate) by the dutyholder. This information should be made available for operational experience and trending analysis.

Table 4 – Guidance on NISR 2003 Regulation 18 Reporting

ONR Category	Description
Major	Incursions or other malicious activity conducted against the transport; or, where all key control measures necessary to satisfy the delivery of security outcomes and relevant good practices have been, or are likely to be, compromised, which could result in a serious consequence.
Moderate	Where one or more key control measures necessary to satisfy the security outcomes or relevant good practice have been significantly weakened, which could result in a significant consequence.
Minor	Where the key control measures necessary to satisfy security outcomes and relevant outcomes remain broadly effective but could result in a minor consequence.
None	Where there has been an event or matter that has no security affect or consequence.

Regulation	Description
18	*(a) any unauthorised incursion on to, interference with, or other incident affecting the security of any means of conveyance of Category I/II nuclear material or Category III nuclear material during the course of its transport or any attempted or suspected such incursion, interference or incident;* *(b) any unauthorised incursion on to premises where Category I/II nuclear material or Category III nuclear material is being stored temporarily during the course of or incidental to its transport or any attempted or suspected such incursion;* *(c) any incident occurring during the transport of Category I/II nuclear material or Category III nuclear material, or on premises where such material is being stored temporarily during the course of or incidental to its transport, involving an explosive or incendiary device or suspected such device, or a firearm or replica firearm;* *(d) any damage to the means of conveyance of Category I/II nuclear material or Category III nuclear material which might affect the security of that material;* *(e) any damage to any building or equipment on premises where Category I/II nuclear material or Category III nuclear material is*

Regulation	Description
	being stored temporarily during the course of or incidental to its transport which might affect the security of the material; *(f) any theft or attempted theft, or any loss or suspected loss, or any unauthorised movement of, or any interference with, Category I/II nuclear material or Category III nuclear material during transport;* *(g) any theft or attempted theft, or any loss or unauthorised disclosure, of information falling within regulation 16(2)(c), or any suspected such theft, loss or disclosure;* *(h) any unauthorised access to any such information or any attempt to gain such access;* *(i) any threat to do anything which would fall within any of sub-paragraphs (a) to (h);* 1.Typical **Major** examples might include: a. Any act or attempted act of sabotage to security assets protecting nuclear material in transit, including by cyber-attack (e.g., escort). b. Confirmed incursion into any location where a transporter and nuclear material is being temporarily stored. c. Any act or attempted act of sabotage of sabotage against nuclear material in transit or its associated transport facilities/equipment (e.g., HSV, locomotive) d. Any theft or attempted theft of nuclear material during a transport or while in temporary storage, or SNI relating to a transport. e. Any protest that blocks the ongoing movement of Category I/II nuclear material in a way that CNC's ability to achieve PPS Outcome is, or is likely to be, compromised. f. Confirmed compromise of information classified as SECRET or above (e.g., highly detailed and exploitable information regarding nuclear material in transit that may jeopardise an effective nuclear security response; or that which could seriously damage international relations) g. Confirmed compromise of operational technology involved in the transport of nuclear material that is categorised as 'Critical' or 'Major' impact. h. Confirmed compromise of IT and/or associated network(s) handling information concerning the transport of nuclear material that is security classified as SECRET or above. 2.Typical **Moderate** events might include: a. Attempted attack or incursion onto a transporter carrying nuclear material.

Regulation	Description
	b. Attempted entry into a location where nuclear material is being stored. c. Any protest that blocks the ongoing movement of Category I/II nuclear material but does not significantly impact CNC's ability to deliver PPS Outcome. d. Any protest that successfully blocks the ongoing movement of Category III nuclear material. e. Malicious damage to any transporter or associated equipment while material is in transport. f. Confirmed compromise of information classified as OFFICIAL SENSITIVE:SNI (e.g., information likely to be of minimal consequence to nuclear security if lost, stolen or published in the media) g. Confirmed compromise of operational technology involved in the transport of nuclear material that is categorised as 'Significant' or 'Minor' impact. h. Confirmed compromise of IT and/or associated network(s) handling information concerning the transport of nuclear material that is security classified as OFFICIAL SENSITIVE:SNI. 3.Typical **Minor** events might include: a. Any attempt to block by protest any movement of Category III nuclear material. b. Attempt to gain unauthorised access. c. Attempt to cause malicious damage or disrupt a transport. d. Unsuccessful attempt by protestors to block the ongoing movement of category I/II and Category III nuclear material e. Significant anomalous activity or indicator of compromise identified on operational technology involved in the transport of nuclear material requiring further investigation (confirmation of compromise would necessitate an uplift in event grading). f. Significant anomalous activity or indicator of compromise identified on IT and associated networks handling SNI concerning the transport of nuclear material that requires further investigation (confirmation of compromise would necessitate an uplift in event grading). g. A reasonable suspicion of the loss or compromise of information that is reportable in accordance with the Collaboration on Gas Centrifuge Technology Handbook on Security of Classified Information, that requires further investigation (confirmation of compromise would necessitate an uplift in the event grading).

Regulation	Description
18	*(j) any failure to comply with any of the standards, procedures and arrangements described in the approved carrier's approved transport security statement or the measures described in any approved transport plan required under regulation 19;* 1.Typical **Major** examples might include: a. Pass (and PIN) handed to another individual in order to gain access to a transport of where material is temporarily stored for malicious purposes b. Use of unapproved stabling or overnight storage arrangements that could result in loss or sabotage of material in transport c. Inability to activate all elements of the emergency/contingency arrangements. d. Movement of Category I/II nuclear material without submitting a Transport Security Plan. e. Total loss of any Security Management System covering the transport, or while material is temporarily stored. 2.Typical **Moderate** events might include: a. Visitors left unescorted within the secure 'bubble' of a transport or where material is temporarily stored. b. Breaches of procedure in the arrangements to protect information security classified as SECRET or above. c. Security boundary door found insecure, and alarm inhibited d. Non-compliance with search regime at any stage of a transport e. Pass (and PIN) handed to another individual in order to gain access to a transport of where material is temporarily stored f. Pass issued to someone involved in a transport who does not hold the correct clearance g. Use of unapproved stabling or overnight storage arrangements h. Inability to activate some element of the emergency/contingency arrangements. i. Not submitting a 7-day notification for movement of Category III nuclear material j. Loss of a significant proportion of any security management system covering a transport or while material is stored for periods of more than four hours. 3.Typical **Minor** events might include: a. Visitors left unescorted in the vicinity of the secure 'bubble' of a transport or where material is temporarily stored b. Breaches of procedure in the arrangements to protect information security classified as OFFICIAL-SENSITIVE:SNI (e.g., sending over the internet unencrypted).

Regulation	Description
	c. Non-compliance with search regime for a transport d. Inability to activate some element of the emergency/contingency arrangements e. Use of non-approved rest area during a Cat III transport. f. Failure of a minor element of any security management system covering a transport or while material is temporarily stored for periods sin excess of four hours.
18	*(k) any other event or matter which might affect the security of—* *(i) Category I/II nuclear material or Category III nuclear material being transported,* *(ii) premises where Category I/II nuclear material or Category III nuclear material is being stored temporarily during the course of or incidental to its transport, or (iii) any information falling within regulation 16(2)(c).* 1. Typical **Moderate** events might include: c. Discovery of prohibited items in location associated with transportation of nuclear material. d. Large, organised protest or gathering in proximity to nuclear transport. 3.Typical **Minor** events might include: f. Attempt to bring prohibited items onto location associated with transportation of nuclear material. g. Discovery of lost or mislaid pass on-site h. Member of public filming or acting suspiciously in proximity to nuclear material transport. i. Acts of criminality indicating staff (involved in transportation of nuclear material) behaviours of concern regarding honesty and integrity.

8.7. Regulation 19 – Duties relating to particular transports of Category I/II Nuclear Material

(1) No Class A carrier shall transport any Category I/II nuclear material unless a transport plan relating to the particular transport by him has been approved by the ONR.

(2) No less than one month before the proposed date on which the transport of any Category I/II nuclear material is to begin (whether or not the transport is to be undertaken in stages by more than one carrier), each Class A carrier who is to transport the material must submit a transport plan relating to the transport by him for the approval of the ONR.

(3) The transport plan must describe in writing the measures to be adopted to ensure the security of the material during—

(a) the course of the transport,

(b) the loading or unloading of the material during the course of or incidental to the transport, and

(c) any period of temporary storage during the course of or incidental to the transport.

(4) The ONR may approve the transport plan as submitted or with such amendments as the ONR may require.

(5) Before approving such a plan the ONR must—

(a) consult the responsible person in relation to any nuclear premises to or from which the material is to be transported and any other Class A carrier who is to undertake another stage of the transport of the material, and

(b) consider any representations made by them.

(6) Each Class A carrier must ensure that any particular transport of Category I/II nuclear material by him conforms to the transport plan approved by the ONR in relation to that transport.

7) No less than 7 days before the proposed date on which any Class A carrier is to begin transporting any Category I/II nuclear material, he must give notice in writing to the ONR of the dates on which the transport by him is to begin and end.

165. Inspectors should remind approved carriers to submit their TptSP to ONR for approval at least one month prior to the planned movement, regardless of whether a transport is carried out in stages or as one complete move, each approved Class A carrier must submit a plan for their part in the movement.

166. Each Class A approved carrier must detail their responsibilities within the movement and how they will transfer their security responsibilities to the next approved carrier if appropriate and then to the consignee.

167. The plan must also describe the measures carriers will take to ensure the security of the material during the course of the transport; loading and unloading during the course of, or incidental to, the transport; and any period of temporary storage during the course or incidental to the transport.

168. ONR may approve the plan as submitted or with such amendments as ONR requires.

169. Before approval of the TptSP ONR will consult the responsible dutyholder for any nuclear premises to or from which the nuclear material is to be transported and any other Class A carrier who is undertaking another stage of transport and consider any comments made by them as they affect ONR's assessment of the TptSP.

170. Inspectors should be aware that prior to a movement of Category I/II nuclear material, the Transport Security Principal Inspector will inform the relevant CNSS duty inspectors that a move is taking place within their duty period.

8.8. Regulation 20 - Duties relating to particular transports of Category III Nuclear Material

(1) Subject to paragraph (3), no less than 7 days before the proposed date on which any approved carrier is to begin transporting any Category III nuclear material, he must give notice in writing to the ONR of the matters specified in paragraph (2) in relation to the transport by him.

(2) The matters are—

(a) the dates on which the transport is to begin and end,

(b) the places from which and to which the material is to be transported,

(c) the identity of the persons from whom and to whom the material is to be transferred,

(d) where all or any part of the transport is to take place outside the United Kingdom, the route of the transport,

(e) any places at which the material is to stop temporarily, and

(f) where the material is to be transported otherwise than in a closed and locked vehicle, railway compartment or shipping compartment, details of the container to be used to transport the material.

(3) In exceptional circumstances notice under paragraph (1) may be given less than 7 days before the proposed date on which the approved carrier is

to begin transporting the material, but a notice that is so given must specify what the exceptional circumstances are.

(4) Where an approved carrier gives notice as mentioned in paragraph (3), he must obtain approval from the ONR for the transport of the material by him before he begins transporting it.

(5) This regulation does not apply to a carrier who transports a vehicle carrying nuclear material on his ship to or from the United Kingdom if the driver of the vehicle drives it on and off the ship and remains on the ship during the ship's journey.

171. Inspectors should be aware that in exceptional circumstances less than seven days' notice may be given but the specific reasons must be given in the notification to ONR. The approved carrier must have approval from ONR before commencing transport of the material. Inspectors should be aware that CNSS transport inspectors will make a judgement on the reasons provided for the delay e.g., poor weather affecting a movement by ship or mechanical breakdown of a road transport. These are exceptional circumstances but an approved carrier omitting to inform ONR in a timely manner is not.

172. The approved carrier must provide the following details in relation to the movement of the nuclear material:

a. The dates on which the transport is to begin and end.

b. The place from where and location to which the material is to be transported.

c. The identity of the persons from whom (Consignor) and to whom (Consignee) the material is to be transferred.

d. Where all or any part of the transport is to take place outside of the United Kingdom, the route the transport will take.

e. Any places where the material is to temporarily stop, and;

f. Where material is to be transported other than in a closed and locked vehicle, railway compartment or shipping container, details of the container to be used to transport the material.

173. Inspectors should be aware that his regulation does not apply where the carrier is the operator of a roll-on-roll-off ferry, and the driver drives the vehicle on and off the vessel.

8.9. Regulation 21 – Directions to Carriers

(1) An approved carrier must comply with any direction given by the ONR for the purpose specified in section 77(1) of the 2001 Act relating to his

business as a carrier of Category I/II nuclear material or Category III nuclear material and requiring the approved carrier—

(a) not to begin a particular proposed transport,

(b) to adopt or implement standards, procedures or arrangements specified in the direction and to secure that his officers, employees, contractors and consultants comply with them,

(c) to submit a fresh transport security statement or amendments of his approved transport security statement,

(d) to satisfy the ONR about the continuing or future adequacy of his approved transport security statement, or that he is complying with it,

(e) to record or investigate in such manner as is specified in the direction—

(i) any event or matter of a kind specified in regulation 18(5), or (ii) any such other event or matter as is specified in the direction, or to report, in such manner as is specified in the direction, to the ONR, or such other person as is so specified, any such other event or matter as is so specified, or

(f) to take such steps as the ONR considers necessary to remedy or alleviate the consequences of any contravention of these Regulations.

(2) Such a direction may impose a requirement to be met—

(a) within a period specified in the direction, or

(b) in the case of a direction under paragraph (1)(d), periodically at such intervals as are specified in the direction.

3) Any direction given by the ONR to a carrier on or after 1st April 2014 under paragraph (1)—

(a) is subject to any 2001 Act direction given to the carrier whenever given; and

(b) must state that it is subject to any such 2001 Act direction.

174. NISR 2003 Regulation 21(1) specifically relates to an approved carrier and the requirement for the responsible person to comply with any direction given by ONR in respect of security standards, procedures and arrangements for the transport of Category I/II nuclear material or Category III nuclear material. Directions might require responsible persons to:

a. Cancel a proposed transport

b. Modify a specific aspect of the extant transport security arrangements and ensure the change is complied with - e.g., vulnerability has been

identified during inspection which requires to be addressed. Whilst ONR would seek to influence improvements, dutyholder inaction or attitude may require a more formal enforcement action to ensure appropriate resolution. ONR inspectors should refer to the ONR EMM for further guidance (Ref. 1).

c. Submit a new TSS or TptSP for approval in accordance with Regulation 16(5), - This might be required in response to ONR's concerns regarding the currency of the plan as a consequence of changes to the DBT or transport operations that invalidate the basis of the security plan.

d. Confirm the extant TSS/TptSP is fit for purpose, and they are compliant with it – ONR's expectation detailed in SyAPs is that security plans will be subject to periodic reviews. This is important to ensure that small iterative changes are considered as a collective whole and that the dutyholder takes into account changes in relevant good practice. It should be noted that such a review may require amendments to be submitted in accordance with Regulation 16(5).

To:

i. Record or investigate an event covered by Regulations 18(5) or as specified in the Direction;

ii. Provide a report in accordance with the Direction;

iii. Take whatever steps ONR considers necessary to correct or mitigate any non-compliance with the extant TSS/TptSP. This is extremely broad and powerful and should always be subject to the principles of the Regulators Code.

175. Unlike an improvement or prohibition notice issued under the HSWA 1974, inspectors should note that dutyholders have no recourse of appeal to a tribunal against a direction. Dutyholders nevertheless do have the right to judicial review. However, it should be noted that similar to a prohibition notice, security directions have legal effect from the time of issue rather than being placed on hold pending the outcome of any review.

176. A judicial review is where a High Court Judge sitting in the Administrative Court considers whether an action or decision of a public authority is lawful. They are normally looking at either:

iii. whether a public authority has properly followed the policies it has in place; or sometimes, more broadly,

iv. whether the policy itself is unlawful in some way.

177. The procedure initially involves a Claimant (or their legal representative) sending a pre-action letter, which gives the public authority a chance to resolve the cases where a mistake may have been made by the person making the decision. But if the public authority stands by its policy/decision, proceedings may be started, and the court will decide whether it is unlawful.

Generally, where the court finds in favour of the Claimant, the remedy is an instruction to the public authority to retake the decision properly/fairly, or to reconsider the policy it has in place and replace it with a different one which is not unlawful. The court normally does not substitute the public authority's decision with its own decision (or policy), so in that respect it is different to an appeal to a Tribunal where a new decision is often simply imposed.

178. Regulation 21(2) enables ONR to place a time limit on meeting a direction or, where confirmation of continuing compliance is required, the periodicity of progress reports. Examples could include monitoring the progress of security improvement schedule projects or other major changes. However, ONR's regulatory approach is for influencing and enabling to be exhausted before formal enforcement action is taken.

179. Template directions are available on HOW2 under 'Templates and Forms'.

9. NISR Part 4 – Security of Sensitive Nuclear Information and Uranium Enrichment Software and Equipment

9.1. Regulation 22 - Regulation of Sensitive Nuclear Information, Uranium Enrichment Equipment and Software

180. As stated previously, NISR 2003 Regulation 4 requires nuclear premises to have an approved security plan which sets out how the dutyholder will protect sensitive nuclear information (SNI) and, if applicable, uranium enrichment software and equipment.

181. Inspectors should be aware that whilst Regulation 4 applies only to nuclear premises, those duty holders are likely to hold SNI at locations outside of their nuclear premises; such as in head offices or other administration buildings. On many occasions, SNI may also be shared with third parties such as their supply chain. Under these circumstances, the protection of SNI is regulated under Regulation 22 of NISR 2003. There are also other dutyholders who produce, store and control their own SNI, such as CNC and NDA, who are also subject to this regulation.

22(1) Subject to the exceptions in paragraphs (2), (3) and (6) this regulation applies—

(a) to any person who has possession or control of sensitive nuclear information in the United Kingdom and who is involved in the following activities—

(i) activities on or in relation to a nuclear site or nuclear premises or who is proposing to become so involved;

(ii) the enrichment of uranium (whether in the United Kingdom or elsewhere); or

(iii) activities with a view to, or in connection with, the enrichment of uranium (whether in the United Kingdom or elsewhere); and

(b) to any person who has possession or control of uranium enrichment equipment or uranium enrichment software in the United Kingdom and who is involved or proposing to become involved in the following activities (whether in the United Kingdom or elsewhere)—

(i) the enrichment of uranium;

(ii) activities with a view to, or in connection with, the enrichment of uranium; or

(iii) the production, storage or transport of equipment or software on behalf of a person involved in the activities mentioned in sub-paragraph (i) or (ii).

182. Regulation 22(1) sets out that the Regulation applies to any person who has in their possession or control, SNI and is involved in, or proposing to become involved in, one of the following activities:

a. activities on or in relation to a nuclear site or nuclear premises or who is proposing to become so involved;

b. the enrichment of uranium (whether in the United Kingdom or elsewhere); or

c. activities with a view to, or in connection with, the enrichment of uranium (whether in the United Kingdom or elsewhere).

183. This means that uranium enrichment technology, even if the enrichment takes place in another country, would be subject to this regulation when information, software or equipment is present in the UK.

22(2) This regulation does not apply—

(a) to an approved carrier insofar as the security of the sensitive nuclear information that he has in his possession is the subject of an approved transport security statement or an approved transport plan; or

(b) to any person, insofar as the information he has in his possession or control has previously been made available to the public anywhere in the world otherwise than in contravention of section 80(3) of the 2001 Act or of any other prohibition breach of which was an offence at the time when it was so made available (including, in a case in which it was made available outside but not within the United Kingdom, an offence under the law of one or more of the places where it was made available).

184. Regulation 22(2) specifies when the Regulation does not apply detailing the following:

a. to approved carriers (as they are subject to Regulation 16 and will be regulated in line with their approved Transport Security Statement and Transport Security Plan); or,

b. to information that has previously been made publicly available and would not be subject to any prior criminal charges for release of the information.

22(3) Subject to paragraph (2) paragraph (1)(a)(i) applies to a person only to the extent that he knows that the information in his possession or

control is or should have been protectively marked, or was so marked when he received it, but a person listed in paragraph (4) cannot benefit from this exception.

185. Regulation 22(3) further identifies that the person in possession or control of the information must reasonably know that the information was protectively marked or should have been protectively marked. This would prevent individuals such as couriers being subject to the Regulation when they are delivering an unmarked letter containing SNI.

22(4) The exception in paragraph (3) does not apply to a person who—

(a) is a responsible person who keeps such information on any premises other than nuclear premises for which there is an approved security plan;

(b) has possession or control of such information for the purposes of planning, designing, or constructing any proposed nuclear premises or installation or other facility on nuclear premises;

(c) is the Nuclear Decommissioning Authority or has possession or control of such information for purposes related to the discharge by the Nuclear Decommissioning Authority of responsibilities given to it by designation under section 3 or 4 of the Energy Act 2004;

(d) is any contractor or consultant of any person referred to in sub-paragraphs (a) to(c);

(e) is a holding company (as defined in section 736(1) of the Companies Act 1985) whose subsidiary (as defined in that section) falls within any of sub-paragraphs (a) to (d); or

(f) is a subsidiary (as defined in section 736(1) of the Companies Act 1985) of a person falling within sub-paragraph (e).

186. Regulation 22(4) caveats that the exception found in Regulation 22(3) does not apply where the person in question clearly should have knowledge of the information's value and the requirement to mark and protect it accordingly. This list includes Regulation 4 dutyholders in relation to their Regulation 22 sites, their employees and contractors, the Nuclear Decommissioning Authority and holding companies or subsidiaries of other NISR 2003 dutyholders.

22(5) For the purposes of paragraph (3)—

(a) information is protectively marked if it bears a protective marking—

(i) which complies with the requirements of the classification policy; [or]

(ii) […]

(iii) which has been applied by the [ONR] or a statutory body in the interests of national security;

(b) information should have been protectively marked if such marking was required by the classification policy.

187. Regulation 22(5) clarifies the definition of protectively marked information to include that which has been marked in line with the ONR classification policy or should have been marked in line with that classification policy. It also includes, in Regulation 22(5)(a)(iii) information that has been protectively marked by ONR or another Statutory Body in the interests of national security. This would include information such as threat intelligence shared by HMGs security agencies. Such information would fall under this Regulation, when in the possession of a person subject to the Regulation.

188. Inspectors should note that SNI is defined in three separate pieces of legislation and as such, whilst not taking precedence over legislation, a simple working definition is provided within the ONR Classification Policy. All three legal definitions are also presented within the Classification Policy at http://www.onr.org.uk/cnss/index.htm

22(6) This regulation applies to a responsible person only to the extent that he keeps sensitive nuclear information or uranium enrichment equipment or uranium enrichment software in premises other than premises for which there is an approved security plan.

189. Regulation 22(6) confirms that premises subject to Regulation 4 are not subject to Regulation 22 (as they will be regulated in line with the applicable Site Security Plan).

22(7) A person to whom this regulation applies must—

(a) maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within his possession or control;

190. Inspectors should note that this is an absolute statement and does not easily align with the principle of proportionality, found within the Regulators Code. To address this issue, ONR has implemented a proportionate regulatory methodology with ‘evidencing expectations’ aimed at Regulation 22 duty holders. The methodology categorises duty holders into one of four inherent risk profiles based upon a series of questions regarding the duty holder’s physical and electronic holdings of SNI. The expectations that the dutyholder is required to evidence are aligned to their risk profile. All expectations contained within the methodology align to SyAPs and the supporting TIGs and TAGs. Accordingly, ONR’s SyAPs, TIGs and TAGs are considered to be relevant good practice against which compliance with Regulation 22 will be judged. However, it is recognised that SyAPs is broader than Regulation 22

vires. Fig. 1 details those elements of SyAPs which apply to these dutyholders. Copies of the evidencing expectations and the inherent risk profile questionnaire can be found on the ONR website.

191. Inspectors should note that where a Regulation 22 dutyholder has other sites that are subject to an approved security plan, the dutyholder may wish to expand the scope of the plan to include their Regulation 22 sites. In such circumstances, their Regulation 22 sites will be regulated against the arrangements contained within their approved plan, rather than the 'evidencing expectations' document.

> *22(7)(b) comply with any directions given by the **[**ONR**]** requiring him to take such steps as are necessary or as are specified in the direction for that purpose;*

192. Regulation 22(7)(b) requires dutyholders to comply with any direction given by ONR. Refer to ONR EMM for further guidance on issuing directions. Unlike an improvement or prohibition notice issued under the HSWA 1974, inspectors should note that dutyholders have no recourse of appeal to a tribunal against a direction. Dutyholders nevertheless do have the right to judicial review. However, it should be noted that similar to a prohibition notice, security directions have legal effect from the time of issue rather than being placed on hold pending the outcome of any review.

193. A judicial review is where a High Court Judge sitting in the Administrative Court considers whether an action or decision of a public authority is lawful. They are normally looking at either:

a) whether a public authority has properly followed the policies it has in place; or sometimes, more broadly,

b) whether the policy itself is unlawful in some way.

194. The procedure initially involves a Claimant (or their legal representative) sending a pre-action letter, which gives the public authority a chance to resolve the cases where a mistake may have been made by the person making the decision. But if the public authority stands by its policy/decision, proceedings may be started, and the court will decide whether it is unlawful. Generally, where the court finds in favour of the Claimant, the remedy is an instruction to the public authority to retake the decision properly/fairly, or to reconsider the policy it has in place and replace it with a different one which is not unlawful. The court normally does not substitute the public authority's decision with its own decision (or policy), so in that respect it is different to an appeal to a Tribunal where a new decision is often simply imposed.

> *22(7) (c) ensure that each of his relevant personnel who is involved in any of the activities listed in any of the paragraphs to sub-paragraph (a) or (b) of paragraph (1) is familiar with the security standards, procedures and arrangements mentioned in paragraph (7)(a) or steps specified in any direction given under paragraph (7)(b) relevant to that activity;*

(d) ensure that each of his relevant personnel who—

(i) is specified in a direction given under paragraph (7)(b) as a person whose suitability requires investigation and assessment […] ; or

(ii) falls within a description of persons who are so specified,

is a person who has been [assessed, in accordance with a process that has been approved by the ONR, to be] of suitable character and integrity, having regard to the need to ensure the security of any sensitive nuclear information, uranium enrichment equipment or software within the possession or control of the person to whom this regulation applies; and

195. Regulation 22(7) (c) requires dutyholders to ensure that their employees are fully informed regarding the security arrangements in place to comply with Regulation 22(7) (a) or any specific arrangements required to comply with an ONR Direction relating to Regulation 22(7) (b).

196. Regulation 22(7) (d) place duties on the responsible person to ensure that their relevant personnel have been assessed and found to be of "suitable character and integrity". The process for assessment of relevant personnel must be compliant with the outcomes set out within SyAPs Fundamental Principle 8 and the guidance that underpins it.

22(7) (e) report to the [ONR] any event or matter of a kind specified in paragraph (10) that

relates to any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within his possession or control as soon as practicable and in any event within 24 hours of its becoming known to him, specifying the nature of the event or matter and, in the case of any event, the date and time it occurred and the apparent reason for it.

22(8) If it is not possible for the person in question to make a written report under paragraph (7)(e) within the period specified in that paragraph, he must make the report orally and confirm it in writing within 48 hours of the event or matter becoming known to him.

22(9) In any other case the report must be made in writing.

197. Inspectors should be aware that Regulation 22(7)(e), (8), (9) and (10) relate to the reporting of security events to ONR. In line with Regulation 10, incidents should be reported 'as soon as is practicable' and in any event within 24 hours of becoming aware of the event. If a written report cannot be provided within that time scale then a verbal report must be made, followed by a written report being made within 48 hours of the event becoming known to them. Further

information on ONR's incident reporting process can be found at [13] and on the ONR website.

22(10) The events and matters are—

(a) any theft or attempted theft, or any loss or unauthorised disclosure of sensitive nuclear information, uranium enrichment equipment or uranium enrichment software, or any suspected such theft, loss or disclosure;

(b) any unauthorised access to sensitive nuclear information, uranium enrichment equipment or uranium enrichment software, or any attempt to gain such access;

(c) any other event or matter which might affect the security of any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software.

198. Regulation 22(10) lists the events that must be reported to ONR examples of which can be found in Annex Z.

22(11) In proceedings for an offence under regulation 25 in relation to this regulation, it is a defence for the accused to show that he is a member of the relevant personnel of another person to whom this regulation applies and that he was acting under the instruction of that other person at the time of the alleged offence.

199. Inspectors should be aware that Regulation 22(11) provides a defence to those in breach of the legislation. It states that if the person in breach of the regulation can show that they are "a member of the relevant personnel of another person to whom this regulation applies and that he was acting under the instruction of that other person at the time of the alleged offence".
The purpose of this defence is to protect employees who are in breach of the legislation as a result of following the direct instructions of their employer.

Table 5 – Guidance on NISR 2003 Regulation 22 Reporting

ONR Category	Description
Major	Incursions into areas holding SNI or any other malicious activity conducted against the premises affecting the security of SNI; or, where all key control measures necessary to satisfy the delivery of security outcomes and relevant good practices have been, or are likely to be, compromised, which could result in a serious consequence.
Moderate	Where one or more key control measures necessary to satisfy the security outcomes or relevant good practice have been significantly weakened, which could result in a significant consequence.
Minor	Where the key control measures necessary to satisfy security outcomes and relevant outcomes remain broadly effective but could result in a minor consequence.
None	Where there has been an event or matter that has no security affect or consequence.

Regulation	Description
22 (10)	*The events and matters are—* *(a) any theft or attempted theft, or any loss or unauthorised disclosure of sensitive nuclear information, uranium enrichment equipment or uranium enrichment software, or any suspected such theft, loss or disclosure;* *(b) any unauthorised access to sensitive nuclear information, uranium enrichment equipment or uranium enrichment software, or any attempt to gain such access;* *(c) any other event or matter which might affect the security of any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software.* 1. Typical **Major** examples may include: a. Confirmed compromise of information classified as SECRET or above (e.g highly detailed and exploitable information regarding Cat I-III nuclear material or vital areas that may jeopardise the nuclear security response at a nuclear premises or of the nuclear material in transit; or that which may damage international relations) b. Confirmed compromise of IT and/or associated network(s) holding information security classified as SECRET or above.

Regulation	Description
	c. Total loss of security management system in place to protect information security classified as SECRET or above. . 2.Typical **Moderate** events may include: a. Breaches of procedure in the arrangements to protect information security classified as SECRET or above. b. Confirmed compromise of information classified as OFFICIAL-SENSITIVE:SNI (e.g., information likely to be of minimal consequence to nuclear security if compromised; or that which could have other damaging consequences if lost, stolen or published in the media). c. Significant loss of security management system or controls in place to protect information security classified as SECRET or above. d. Total loss of security management system or controls in place to protect information security classified as OFFICIAL-SENSITIVE:SNI. e. Confirmed compromise of IT and/or associated networks handling information classified as OFFICIAL-SENSITIVE:SNI. f. Access to SNI by an individual without the correct level of national security vetting. g. Individuals sharing passes or passwords to allow unauthorised access to SNI, areas or IT/Networks handling SNI. 3.Typical **Minor** events may include: a. Breaches in procedure in the arrangements to protect information security classified as OFFICIAL-SENSITIVE:SNI (e.g., email over the internet without adequate encryption) b. Significant anomalous activity or indicator of compromise identified on IT and/or associated networks handling SNI that requires further investigation (confirmation of compromise would necessitate an uplift in the event grading) c. Criminal conviction of a Director/Board member of a Regulation 22 dutyholder. d. Loss of an asset handling SNI that is suitably encrypted (e.g., FOUNDATION grade for OFFICIAL-SENSITIVE:SNI) e. The foreign takeover of a Regulation 22 dutyholder. f. The compromise of a dutyholder's website. f. A break in to a List N premise, without a known compromise to SNI held there. g. A reasonable suspicion of the loss or compromise of information that is reportable in accordance with the

Regulation	Description
	Collaboration on Gas Centrifuge Technology Handbook on Security of Classified Information, that requires further investigation (confirmation of compromise would necessitate an uplift in the event grading).

10. NISR Part 5 – General and Supplementary Provisions

10.1. Regulation 25 – Offences

(1) If any person fails to comply with any provision of regulation 4(1), 5, 7, 8, 9, 10, 11, 12, 13, 17, 18, 19, 20, 21, or 22, he shall be guilty of an offence.

(1A) For the purposes of paragraph (1), a person is not to be regarded as failing to comply with any provision mentioned in that paragraph by reason of anything done, or omitted to be done, by that person in order to comply with a 2001 Act direction.

(2) A person guilty of an offence is liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine (or both), and

(b) on summary conviction, to imprisonment for a term not exceeding six months or a fine (or both).

(2A) In Scotland and Northern Ireland, a fine imposed under paragraph (2)(b) may not exceed the statutory maximum.

(3) Proceedings for an offence to which paragraph (2) applies that is committed outside the United Kingdom may be taken, and the offence may for incidental purposes be treated as having been committed, in any place in the United Kingdom.

200. Inspectors should be aware that NISR 2003 Regulation 25 establishes offences should a responsible person fail to comply with any provision of, Regulations 4(1), 5, 7, 8, 9, 10, 11, 12, 13, 17, 18, 19, 20, 21, or 22.

201. Regulation 25 (1A) provides a defence to those in breach of the legislation. Section 77(1 - 4) of that Act, being primary legislation, defines what the Secretary of State may include in their regulations for the purposes of regulation of security in the civil nuclear industry. The directions contained in Section 77(1- 4) covers all the purposes of security regulation contained within NISR 2003 (site, nuclear material and ORM on nuclear sites, equipment and software connected with uranium enrichment, nuclear construction sites, transport of nuclear material off nuclear sites, the protection of sensitive nuclear information) therefore to use this defence, the dutyholder has to demonstrate how their action, inaction or omission was in compliance with a 2001 Act direction. In effect the 2001 Act empowers the Secretary of State to make nuclear security regulations under which NISR 2003 were originally laid prior to transfer to become a Relevant Statutory Provision of TEA 2013.

202. Regulation 25 also defines the offence punishment scale if the person is found guilty of an offence, further specifying that if the offence is proven in Scotland or Northern Ireland any fine may not exceed the statutory maximum.

203. Regulation 25(3) also establishes offences committed outside the United Kingdom may be treated as having been committed in any place in the United Kingdom. For example, a memory stick lost abroad containing O-S:SNI may be considered an offence committed in the UK.

10.2. Regulation 25A – Notification of Compliance with a 2001 Act Direction

(1) Where a person to whom these Regulations apply—

(a) is required to comply with a 2001 Act direction; and

(b) is of the opinion that the person cannot comply both with that direction and any provision of these Regulations (a "relevant provision"), that person must notify the ONR.

(2) A notification under paragraph (1) must—

(a) be given as soon as reasonably practicable;

(b) give details of the relevant 2001 Act direction; and

(c) specify the relevant provision.

204. Regulation 25 (a) states that if the person to whom the 2001 Act applies is of the opinion they cannot comply with both the 2001 Act and NISR 2003, they must notify ONR as soon as is practicable explaining which 2001 Act direction is preventing them complying with the relevant provision of NISR 2003.

10.3. Regulation 26 – Exclusion of Defence Premises and Transports

These Regulations do not apply—

(a) to any nuclear premises controlled or operated wholly or mainly for the purposes of the department of the Secretary of State with responsibility for defence, or

(b) to any transport of nuclear material for the purposes of the department of the Secretary of State with responsibility for defence.

205. Inspectors should note that this does not mean that a contract with the MoD will automatically result in an exclusion being applied. The applicability will be determined by the respective proportions of work undertaken for defence and civil purposes, in consultation with the regulatory bodies concerned.

10.4. Regulation 27A - Transport by a Ship other than a United Kingdom Ship

(1) Subject to the provisions of this regulation, these Regulations do not apply to transport in a ship that is not a United Kingdom ship.

(2) The relevant provisions apply to transport within the United Kingdom or its territorial sea in a ship that is not a United Kingdom ship if the ship—

(a) is proceeding to a port in the United Kingdom in order to enter it, or entering, leaving or proceeding from such a port and is carrying nuclear material, or

(b) is proceeding to such a port for nuclear material to be loaded on to it there.

(3) Paragraph (2) applies to transport in a Government ship only at a time when the ship is being used for commercial purposes.

(4) In their application to transport in a ship that is not a United Kingdom ship the provisions of Part 1 and regulations 18 to 21 of these Regulations apply with the following modifications—

(a) subject to paragraph (5), any obligation imposed by those provisions is to be read as an obligation that must be met in respect of the ship in question as a condition of its entry to the port in question;

(b) in regulations 18, 20 and 21 a reference to "an approved carrier", or "the approved carrier" is to be read as a reference to "a carrier" or "the carrier" (as the case may be);

(c) regulation 18 applies as if in paragraph (5)(j) of that regulation the words from "the standards" to "or" were omitted;

(d) in regulation 19—

(i) subject to paragraph (ii), any reference to a "Class A carrier" is to be read as a reference of to "a carrier";

(ii) the reference to "any other Class A carrier" in paragraph (5)(a) is to be read as a reference to "any other carrier";

(e) regulation 21(1) applies as if sub-paragraphs (c) and (d) were omitted.

(5) Paragraph (4)(a) is without prejudice to the continuation of an obligation in so far as it is capable of remaining operative after a ship leaves the port in question.

(6) For the purposes of this regulation—

(a) "the relevant provisions" are the following provisions of these Regulations—

(i) Part 1;

(ii) regulations 18 to 21;

(iii) this Part;

(b) "Government ship" means a ship which—

(i) is not a United Kingdom ship; and

(ii) is owned by the Government of a country outside the United Kingdom or a department or agency of such a Government.

206. Inspectors should note that Regulations 13-21 do not apply to transport in a ship that is not United Kingdom (UK) flagged. The relevant provisions apply to transport within the UK or its territorial sea, defined as within 12 nautical miles of the coast, in a ship that is not a UK flagged if it is:

a. proceeding to a port in the UK in order to enter it, or entering it, leaving or proceeding from such a port and is carrying nuclear material (it need not be unloading the nuclear material at the UK port for the relevant provisions to apply); or,

b. proceeding to such a port where nuclear material will be loaded on to it.

207. The relevant provisions apply to transport in a government ship only at a time when the ship is being used for commercial purposes.

208. In their (carrier) application to transport in a ship that is not a UK ship the provisions of Part 1 and Regulations 18 to 21 apply with the following modifications:

a. subject to paragraph 5 of Regulation 27 (a) any obligation imposed by these provisions is to be read as an obligation that must be met in respect of the ship in question as a condition of entry to the port in question.

b. In Regulations 18, 20 and 21 references to "an approved carrier" or "the approved carrier" should be read as "a carrier" or "the carrier" respectively.

c. In Regulation 19 references to "Class A carrier" is to be read as "a carrier", further any references to "any other Class A carrier" is to read as "any other carrier"

d. Regulation 21 – Directions to carriers applies as if the 4th and 5th bullet point were omitted.

209. For the purposes of this regulation the “relevant provisions” are the following provisions of these regulations which are:

a. Part 1
b. Regulations 18 to 21
c. This part which falls within part 5 of the regulations.

210. The term government ship means a ship which:

a. is not a UK ship and;

b. is owned by a government of a country outside of the UK or a department or agency of such a government.

11. NISR 2003 – The Schedule

Table 3: Categories of Nuclear Material

MATERIAL	CATEGORIES	
	I/II	III
1. Plutonium (other than plutonium with an isotopic concentration exceeding 80% in plutonium-238) which is not irradiated	More than 500 grammes	500 grammes or less, but more than 15 grammes
2. Uranium-233 which is not irradiated	More than 500 grammes	500 grammes or less, but more than 15 grammes
3. Previously separated neptunium-237 which is not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
4. Previously separated americium-241, previously separated americium-242m or previously separated americium-243, which are not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
5. Uranium-235 in enriched uranium containing 20% or more of uranium-235, which is not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
6. Uranium-235 in enriched uranium containing 10% or more, but less than 20%, of uranium-235, which is not irradiated	10 kilogrammes or more	Less than 10 kilogrammes, but more than 1 kilogramme
7. Uranium-235 in enriched uranium containing less than 10% but more than 0.711% of uranium-235, which is not irradiated		10 kilogrammes or more
8. Irradiated reactor fuel being used, stored or transported within the United Kingdom		Any quantity
9. Irradiated reactor fuel being transported outside the United Kingdom, other than such fuel which, prior to being irradiated, was uranium enriched so as to contain 10% or more, but less than 20%, of uranium-235	Any quantity	
10. Irradiated reactor fuel being transported outside the United Kingdom which, prior to being irradiated, was uranium enriched so as to contain 10% or more, but less than 20%, of uranium-235		Any quantity
11. Other irradiated nuclear material		Any quantity

Table Notes:

"enriched uranium" means uranium enriched so as to contain more than 0.711% of uranium-235;

"irradiated" and "previously separated" have the meanings given in Regulation 3(2).

Further information can be found within paragraph A1.37 – A1.50, SyAPs Annex A and [6].

References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “The Energy Act 2013 C. 32,” 2013.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] H.M. Government, “Nuclear Installations Act 1965 (1965 c.57),” 1965.

[6] ONR, “CNS-TAST-GD-6.1 - Target Identification for Theft”.

[7] ONR, “CNS-TAST-GD-6.2 - Categorisation for Sabotage”.

[8] Cabinet Office, “Government Security Classification (Version 1.1),” HM Government, 2018.

[9] ONR, “CNS-TAST-GD-8.2 - Pre-employment Screening and National Security Vetting”.

[10] ONR, “ONR-DOC-TEMP-103 - ONR Incident Notification Form - INF1”.

[11] ONR, “ONR-ENF-GD-006 - Enforcement”.

[12] ONR, “ONR-PER-IN-006 - Decision Review and Appeals Process”.

[13] ONR, “ONR-OPEX-GD-001 - Notifying and Reporting Incidents and Event to ONR”.

Appendices

Appendix 1 – Advice on Categorisation of Nuclear Material

1. Categorisation is an essential part of determining the applicability of NISR 2003 and implementing a graded approach. Nuclear material varies greatly across the various parts of the nuclear fuel cycle and this appendix provides further context in that regard.

2. Category I refers to types and quantities of nuclear material that require the least effort to fashion into a nuclear explosive device. The lower thresholds (2kg Pu or U233; 5kg U235 in Highly Enriched Uranium (HEU), Am or Np) are intentionally set significantly below the critical mass required to generate a nuclear explosion. However, where dutyholders have a Category I quantity, they tend to have weights far in excess of the lower threshold. For example, Sellafield holds over 120 metric tonnes of plutonium. The term HEU is reserved for uranium that has been enriched to 20% or more U235 in U238. Whilst it is theoretically possible to design a nuclear device at lower enrichments, the technical and practical challenges to overcome due to the increased critical mass (which rises rapidly as enrichment percentage decreases) means that in reality, the threat is not credible.

3. Category II is the maximum categorisation for any quantity of uranium enriched to less than 20% U235. It can also refer to smaller quantities (i.e., subcategory I, refer to the schedule for exact masses) of HEU, U233, Pu, Am or Np. However, these types, forms and weights are extremely rare within the UK nuclear industry. Instead, Category II tends to refer to spent fuel that is destined for international travel or bulk quantities of waste containing nuclear material. Within the UK, fresh fuel for the current generation of power stations consists of Low Enriched Uranium (LEU) up to 5% enrichment.

4. Within a fission reactor using such fuel, the majority of thermal energy is released due to the fission of U235, which produces neutrons that cause fission of further U235 atoms. Where this process becomes self-sustaining then the reactor is said to have achieved criticality. However, in addition to the fission of U235, it is also possible for a U238 atom to absorb a neutron to form Pu239. Pu 239 is also fissile and contributes to sustained criticality; commonly 30% of the thermal energy produced by a conventional reactor comes from the fission of Pu rather than U.

5. The percentage of Pu produced as a result of this irradiation is relatively small (typically around 1% of the total weight of fuel). However, as the fuel is typically stored in large quantities, it contains a quantity of nuclear material (over 200kg spent fuel will contain more than 2 kg of plutonium) sufficient to place it in Category I. However, it is placed within Category II because of its reduced attractiveness due to the high radiation levels it causes and the

associated challenges that poses to machining or processing as described earlier.

6. This document has already described that categorisation is driven by the attractiveness of the material to fashion a nuclear explosive device. Factors such as dilution, dispersion, type and form can all affect the attractiveness of nuclear material for example: Material that is in a dilute form will force an adversary to acquire much larger volumes and masses of material to obtain a significant quantity of nuclear material; material that is part of a homogenous mass, will force an adversary to acquire larger volumes and masses of material to obtain a significant quantity of nuclear material and will pose greater difficulty in identifying and separating the nuclear material from the other less attractive materials; and, the chemical and physical form of the material may have a significant impact because materials that are bound into immobile matrices, such as cementitious grout or a vitrified product, will also create difficulties for adversaries.

7. Where waste containing nuclear material meets these criteria then it is possible for dutyholders to make a case for the categorisation to be reduced in accordance with Table 2 of Annex A to SyAPs. Category II is the maximum categorisation within this table and there are bulk quantities of waste resulting from legacy operations (e.g., weapons and research) that fit within this criterion.

8. Whilst this is the case to determine the applicability of NISR 2003, the regulatory expectation is that quantities above Category III will also be aggregated across isotopes, elements and enrichments. This is important because of the feasibility of constructing a viable nuclear device using a mixture of fissile elements and enrichments. There are several methodologies that can be used to determine the aggregated totals in such circumstances and more information can be found in [6].

Appendix 2 – 7(2) Notification for Reporting of Events or Matters

[Name]
[Title]
[Address line 1]
[Address line 2]
[Address line 3]
[Address line 4]
[Postcode]

Telephone: [ ]
Email: [ ]

Our Reference:[ ]
Unique Number:[ ]

Your Reference:[ ]
Unique Number:[ ]

[Addressee]
[Address]

Date:

NOTIFICATION UNDER REGULATION 7(2) OF THE NUCLEAR INDUSTRIES SECURITY REGULATIONS 2003

Dear,

I acknowledge receipt of your reference **[insert security plan reference]** made under the Nuclear Industries Security Regulations (NISR) 2003, in which you have defined arrangements to categorise and manage events or matters reportable under regulations 10(5)(i) and (j).

NOTIFICATION

In accordance with Regulation 7(2) of NISR 2003, ONR hereby gives notification in writing to **[insert responsible person i.e. the corporate body]** being the responsible person for **[insert nuclear premises name]**, that ONR is of the opinion that the events and matters set out in your reference categorised **[insert reference from security plan]** are unlikely to be prejudicial to the security of the premises and the material, equipment and information mentioned in regulation 4(2). Accordingly, ONR will not regard **[insert responsible person]** as having failed to comply with their approved security plan for such events or matters and a report to ONR under made under Regulation 10 is not required.

Regulatory Expectations:

Your arrangements to categorise and manage events and matters forms part of your security plan or a standalone document suitably referenced from within your security plan and should not be amended without further consideration by ONR.

If you are in any doubt as to whether a matter should be reported to ONR, then you should refer to your nominated site security inspector.

All matters under this category will be recorded by you for ONR sampling as required. If you fail to comply with this notification for any reason, you are required to report the non-compliance to ONR.

Yours faithfully / sincerely

A N Other
Title (e.g., ONR Superintending Inspector – Nuclear Security)

Distribution
A N Other 1, ONR GDA

Appendix 3 – 7(2) Notification for Amending Security Standards, Procedures and Arrangements

[Addressee]
[Address]

[Name]
[Title]
[Address line 1]
[Address line 2]
[Address line 3]
[Address line 4]
[Postcode]

Telephone: [ ]
Email: [ ]

Our Reference:[ ]
Unique Number:[ ]

Your Reference:[ ]
Unique Number:[ ]

Date:

NOTIFICATION UNDER REGULATION 7(2) OF THE NUCLEAR INDUSTRIES SECURITY REGULATIONS 2003

Dear,

In acknowledge receipt of your reference **[insert security plan reference]** made under the Nuclear Industries Security Regulations (NISR) 2003, which defines a categorisation scheme and management of change process for amendments to the standards, procedures and arrangements described, relied upon or referenced in your security plan.

NOTIFICATION

In accordance with regulation 7(2) of NISR 2003, ONR hereby gives notification in writing to **[insert responsible person i.e. the corporate body],** being the responsible person for **[insert nuclear premises name]**, that ONR is of the opinion that the amendments of the type set out in your reference defined as **[insert security plan reference]** are unlikely to be prejudicial to the security of the premises and the material, equipment and information mentioned in Regulation 4(2). Accordingly, ONR will not regard **[insert responsible person]** as having failed to comply with Regulation 7(1) for implementing them prior to ONR approval under Regulation 6(2).

Regulatory Expectations:

In submitting your proposal, you confirm that you are cognisant that the aggregation of a number of proposed changes specified in your reference, conducted concurrently,

may result in an overall change being of a higher significance category and should, therefore, be forwarded to ONR for approval using your defined processes.

You also recognise that all other proposed changes not specified in your Reference will be forwarded to ONR for approval.

Your reference will become either part of an amended security plan or a standalone document suitably referenced from within your security plan. The categorisation scheme and management of change process in your Reference should not be amended further without consideration by ONR.

If you are in any doubt as to the significance category of a change being considered, then you should apply conservatism or refer to your nominated site security inspector.

All changes conducted under this category will be recorded by you for ONR sampling as required. If you fail to comply with this notification for any reason, you are required to report the non-compliance to ONR.

Yours faithfully / sincerely

A N Other
Title (e.g., ONR Superintending Inspector – Nuclear Security)

Distribution
A N Other 1, ONR GDA

Appendix 4 – 8(2) Notification for Temporary Security Plans

[Name]
[Title]
[Address line 1]
[Address line 2]
[Address line 3]
[Address line 4]
[Postcode]

Telephone: [ ]
Email: [ ]

Our Reference:[ ]
Unique Number:[ ]

Your Reference:[ ]
Unique Number:[ ]

[Addressee]
[Address]

Date:

NOTIFICATION UNDER REGULATION 8(2) OF THE NUCLEAR INDUSTRIES SECURITY REGULATIONS 2003

Dear

I acknowledge receipt of your reference **[insert security plan reference]** made under the Nuclear Industries Security Regulations (NISR) 2003, which defines a categorisation scheme and management process for proposed works of alteration or extension to buildings or other structures that for part of your nuclear premises.

NOTIFICATION

In accordance with regulation 8(2) of the NISR 2003, ONR hereby gives notification in writing to **[insert name of responsible person i.e., the corporate body]**, being the responsible person for **[insert nuclear premises]**, that ONR is of the opinion that the proposed works described within your security plan as **[insert relevant excerpt]** are unlikely to be prejudicial to the security of the premises and the material and equipment mentioned in regulation 4(2). Accordingly, regulation 8(1) does not apply to that work, or any work of a description that includes that work and a temporary security plan does not need to be approved by ONR prior to that work commencing.

Regulatory Expectations

In submitting your proposal, you confirm that you have governance procedures in place to assess the scope of all works that fall under Regulation 8(1) and a robust and

consistent methodology has been used to identify the level of risk involved and work graded accordingly. This includes the consequences of the works being inadequately conceived or executed.

A record of all works conducted within this notification category specified in your Reference must be kept for ONR sampling as necessary. All other temporary works that are not defined in your reference should be submitted to ONR under regulations 8(1)(a) and 8(3). If you have any concerns as to the type of works that require notification, please discuss these with your nominated site security inspector.

Yours faithfully / sincerely

A N Other
Title (e.g., ONR Superintending Inspector – Nuclear Security)

Distribution
A N Other 1, ONR GDA