Office for Nuclear Regulation

(Revised: April 2016)

(Version 7.2)

Nuclear Industries Security Regulations 2003 (as amended)

CLASSIFICATION POLICY For the Civil Nuclear Industry

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

Office for Nuclear Regulation

CONTENTS

Page

Part One - Introduction 1

General Principles 1

Applying the Correct Classification 4

Information in the Public Domain 4

Part Two - Abbreviations 5

Section 1. Security of Nuclear and Other Radioactive Material in Use or Storage……6

Section 2. Other Information Relating to Nuclear and Other Radioactive Material in Use or Storage 8

Section 3. Transport Of Nuclear and Other Radioactive Material Within a Nuclear Premises or Between Adjacent Nuclear Premises 9

Section 4. Transport of Nuclear Material Off-Site..... 10

Section 5. Civil Nuclear Constabulary 13

Section 6. Nuclear Material Accounting 14

Section 7. Computer Systems 15

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

PART ONE - INTRODUCTION

General Principles

1. The Nuclear Industries Security Regulations (NISR) 2003 (as amended) require those who operate within the civil nuclear industry to protect Sensitive Nuclear Information (SNI) in an appropriate manner. SNI is defined in the Anti-terrorism, Crime and Security Act 2001 (as amended), as including:

> *"information relating to activities carried out on or in relation to nuclear sites or other nuclear premises which appears to the Secretary of State to be information which needs to be protected in the interests of national security"*

This definition is further amplified in NISR 2003 as including "information which requires a classification in accordance with the classification policy", this policy being defined as "Information concerning the Use, Storage and Transport of Nuclear and other Radioactive Material", issued by the Secretary of State from time to time, and information which bears a classification which has been applied by a Government Department or a statutory body in the interests of national security[1]

2. This policy was formerly known as CWP/G8 Classification Policy. It is now known as the NISR 2003 Classification Policy (NISR CP). The purpose of this policy is to indicate those categories of SNI that require protection and the level of classification to be applied. It is to be implemented in conjunction with the HMG Security Policy Framework.

3. The 2012 Government Security Classification Review detailed that there is no expectation that routine OFFICIAL information will be marked. SNI, is included in the official sensitive subset of OFFICIAL information. This subset covers information that could have more damaging consequences if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but it attracts additional measures to reinforce the 'need to know'. Therefore, SNI assets should be conspicuously marked:

'OFFICIAL–SENSITIVE'
'HANDLE AS SNI'

4. The 2012 Review further detailed that there is no unclassified tier and that all information that is created, collected, processed, stored or shared within government

[1] Extract from Regulation 22(5) of the Nuclear Industries Security (Amendment) Regulations 2006
For the purposes of paragraph (3) -
(a) information is classified if it bears a classification
(i) which complies with the requirements of the classification policy;
(ii) which conforms to the guidelines set out in the document entitled "Finding a Balance: Guidance on the Sensitivity of Nuclear and Related Information and its Disclosure" issued from time to time by the Secretary of State; or
(iii) which has been applied by the Secretary of State or a statutory body in the interests of national security.

(and across the wider Public Sector) has value and requires an appropriate degree of protection even if not explicitly marked as such. It is not practical to compel organisations in the civil nuclear industry to apply the HMG baseline security controls to information they originate which is not SNI. Such information is identified in this document as 'Not SNI'. In some situations it may be appropriate for information originated by organisations that is not SNI, to be positively identified as non-sensitive or commercial.

5. This classification policy, issued by the Office for Nuclear Regulation (ONR) Civil Nuclear Security (CNS), on behalf of the Secretary of State, deals with the classification of information, including that held on IT systems, relating to nuclear facilities, nuclear material and other radioactive material (NM/ORM). This policy includes radioactive sources and material designated as waste. In the interests of national security, a particular objective of this policy is to prevent the disclosure of information which could assist those planning a terrorist act, including theft, sabotage or any other malicious acts. Its application is therefore an integral element in the security of nuclear facilities, NM and ORM. Information covered by this policy falls into two categories:

a. that which concerns the security arrangements to protect nuclear facilities, NM/ORM and;

b. that which covers holdings and movements of NM/ORM, for example, location, stocks, inventories, throughput, output, accounting and transportation.

6. A further purpose of this policy is to define the extent to which information concerning the concept of "material unaccounted for" (Nuclear Material Balance), the actual values of Nuclear Material Balance for NM at particular premises and information on related topics which requires a classification.

7. This document does not deal with technical information about uranium enrichment or the past production or processing of defence NM, as these aspects are dealt with in other classification guides.

8. Policy on the classification of information should not be confused with disclosure policy, or the requirement to protect commercial or other official data. Information that is not classified in accordance with formal policy may nevertheless be sensitive in the context of commercial confidentiality or management issues and should only be released with the approval of an appropriate senior executive.

9. Those to whom this policy applies should be aware of the publication, entitled "Finding a Balance", also issued by ONR (CNS). "Finding a Balance" was produced to offer simple, generalised guidance to a wide audience at unclassified level, largely in relation to enquiries under the Freedom of Information Act 2000 (FOIA). Accordingly, "Finding a Balance", as an informative document, should always be viewed as subordinate to NISR CP.

10. Where there is a requirement to handle, store or transmit any information relating to nuclear facilities or NM/ORM, company or site security plans/instructions

are to be consulted to identify the procedures to be followed to ensure the appropriate level of protection. The Cyber Security and Information Assurance Team at ONR (CNS) may also be able to provide advice if required.

11. It is acknowledged that there will be occasions, for example, during the preparation of Safety or Security documentation, when it may be necessary to include information that attracts a security classification, under the terms of this policy. In these instances originators should consider the use of a separate annex and a limited distribution for such information; to avoid a need to apply a higher classification to the whole document. The test when writing a report should be "Is the addition of specific detail necessary within the scope and purpose of the document? If necessary, can it be included in an annex?"

12. Categories of material referred to in this policy are defined in the NISR 2003 National Objectives, Requirements and Model Standards (NORMS) document[2].

13. Within ONR (CNS), the appointment responsible for the currency and maintenance of this policy is the Superintending Inspector for Cyber Security and Information Assurance, to whom all communications about its purpose and content should be addressed.

14. Although this latest revision has led to the document being downgraded to OFFICIAL, it should be noted that it remains a CIVIL NUCLEAR OFFICIAL document, which should be managed and protected accordingly.

15. This document replaces the previous issue of the NISR Classification Policy, Revision 7.1, dated January 2014, which should now be destroyed.

16. This revised version of NISR CP should be applied in conjunction with related documentation, such as NORMS and HMG Security Policy Framework (SPF) as appropriate.

17. Classifications applied to information being passed to the European Commission under the terms of the Euratom Treaty, should be prefixed "EURA".

18. In cases where it appears necessary to pass classified information to an entity beyond UK jurisdiction, the prefix "UK" should be used. Unless an ONR (CNS) or HMG approved protocol has been established, each instance should be subject to the advice of an appropriately designated person, (e.g. the site security manager) and in some cases the approval of ONR (CNS) before the material is despatched. .

19. Although this policy is concerned primarily with the application of the appropriate classification for current information, consideration should be given to the future requirement for the marking to remain. There are security and administrative benefits in conducting a regular review to consider the need to retain classified material at its original level, which could lead to its downgrading or destruction when no longer required.

[2] NORMS Part One, Annex B, Tables 1 and 2 and Part Two refer.

20. This policy cannot specify separately all of the instances where a declassification timespan may be appropriate. However, this is an area where originators, other specialists and records reviewers should exercise a degree of judgement, according to the sensitivity or timeliness of the information, taking into account the risk management approach outlined below. Site security managers should be consulted in specific instances and the ONR (CNS) Information Security Team may assist when appropriate.

Applying the Correct Classification

21. The originator or nominated owner of information or an asset is responsible for applying the correct classification. When classifying a document where the NISR CP provides a range of classifications, a damage or 'harm test' is to be conducted to consider the likely impact if the asset were to be compromised and to determine the correct level of marking required. The 'harm test' should be carried out by assessing the asset against the criteria for each classification

22. If applied correctly, the Classification System ensures that only genuinely sensitive material is safeguarded. The following points should be considered when applying a classification:

a. Applying too high a classification can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business. Applying too low a classification may lead to damaging consequences and the asset's compromise.

b. The compromise of aggregated or accumulated information of the same classification is likely to have a higher impact. Generally this will not result in a higher classification but may require additional handling arrangements. If the accumulation of that data results in a more sensitive asset being created, then a higher classification should be applied.

c. Sensitivity may change over time, resulting in the need to reclassify information or an asset as appropriate.

Information in the Public Domain

23. For the purpose of this document the phrase "in the public domain" is taken to mean information publicly available irrespective of copyright restrictions that may affect further re-use of that information. It is information that has been published or can be readily acquired by an interested member of the public from a number of sources. However, if information is publicly available and published lawfully, this does not necessarily mean that no classification is required. Each case should be judged on its merits.

PART TWO - ABBREVIATIONS

The following abbreviations are used throughout this policy:

AACS	Automatic Access Control System
ACO	Atomic Control Office
AFO	Authorised Firearms Officer
BRIMS	British Radwaste Information Management System
CCTV	Closed Circuit Television
CNC	Civil Nuclear Constabulary
FOIA	Freedom of Information Act 2000
HEU	High Enriched Uranium
HSV	High Security Vehicle
IAEA	International Atomic Energy Agency
IDS	Intruder Detection System
ILW	Intermediate Level Waste
IT	Information Technology
KMP	Key Measurement Point
LEU	Low Enriched Uranium
LLW	Low Level Waste
MBA	Material Balance Area
NM	Nuclear Material
NORMS	National Objectives, Requirements and Model Standards
Not SNI	Not Sensitive Nuclear Information (not subject to regulation)
NPS	Nuclear Power Station
ONR (CNS)	Office for Nuclear Regulation (Civil Nuclear Security)
ORM	Other Radioactive Material (includes Radioactive Sources)
O-S	OFFICIAL - SENSITIVE
S	SECRET
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
TptSP	Transport Security Plan
TSP	Temporary Security Plan
TSS	Transport Security Statement
VA	Vital Area
VAS	Vessel Alarm Station

SECTION 1. SECURITY OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL IN USE OR STORAGE

1.1 The security plan for a nuclear premises

a.	Premises holding Category I to III NM/ORM and VAs.	S
b.	Premises holding Category IV NM/ORM.	O-S

1.2 A Temporary Security Plan (TSP) for a nuclear premises

a.	A draft or approved TSP which specifies any of the following:	O-S to S
	i. a duration of use.	
	ii. a location.	
	iii. a vulnerability or temporary weakness in the security of NM/ORM.	
	iv. proposed remedial measures.	
	v. compensatory measures to be applied during the TSP period.	

1.3 Vital Areas (VA)

a.	The definition of a VA.	
	IAEA definition.	Not SNI
	NORMS definition.	O-S
b.	The existence of a VA on a site including on NPS.	Not SNI
c.	The location of a VA.	O-S
d.	The protective arrangements for a VA.	S
e.	Information relating to a VA which details vulnerabilities or deficiencies in safety and security that could be exploited for malicious purposes.	S

1.4 Safety cases, engineering documents, and related information

a.	Information that could identify a realistic means of causing a significant radiological release from a plant.	O-S to S
b.	Descriptions of specific, residual and exploitable vulnerabilities in processes, physical structures, systems and essential supporting services designed to control, sustain or contain activities involving NM/ORM.	O-S to S
c.	Information relating to the controls and access to the production process, which reveals detail that could assist those planning the unauthorised removal of NM/ORM from the process area.	
	i. Category I and II.	S
	ii. Category III and IV.	O-S

1.5 Security contingency and response planning

a. The existence of Security Contingency and Response Plans.	Not SNI
b. The detailed content of Security Contingency and Response Plans identifying potential risk events and the planned responses.	O-S to S

1.6 Security and Counter Terrorist (CT) exercises

a. That a site level exercise has been held or is due to take place.	Not SNI
b. The outcome of an exercise and adjustments planned or introduced as a result of shortcomings which may have been revealed in the protection of NM and ORM.	O-S to S

1.7 Security reports

a. Reports of security inspections and other documented reports on the protection of NM/ORM where vulnerabilities are revealed[3].	O-S to S
b. Documented reports or notices showing security deficiencies, knowledge of which could assist persons to by-pass the security arrangements:	
i. Category I, II and III premises, and all VAs.	S
ii. Category IV.	O-S

1.8 Security of nuclear material in use and in storage

Details of construction and layout of stores and process areas, including drawings or plans held on any media, showing features of physical security relevant to the prevention of theft or sabotage of NM/ORM[4]. Cat I, II, III facilities, NPS and VAs:

a. Walls and ceilings - A simple description of a wall, for example that it is concrete or brick but lacking exact detail.	Not SNI
b. Walls and ceilings - If structural details include dimensions such that the level of potential resistance can be assessed.	O-S
c. Doors - The non specific location of doors showing some detail but not explicit information, for example ‘fire door’, or ‘turnstile’.	Not SNI
d. Doors - The location of doors and turnstiles with descriptive detail and specifying whether or not it is alarmed.	O-S
e. Utilities - General reference to utilities simply as water, gas and electricity.	Not SNI

[3] If no vulnerabilities are revealed the report may be Not SNI.

[4] No maps, charts or plans of premises containing descriptions and functions of buildings, or the location of internal security fences and their ancillary equipment, may be published without appropriate management controls. Management decisions on information release should be documented. In appropriate cases advice should be sought from ONR (CNS).

f. Utilities - Reference to utilities that are essential to the functioning of a plant including power supplies for security systems. It must be clear that the services are essential.	O-S to S

1.9 Circuit diagrams or data showing types, configuration and locations of intruder detection system (IDS) sensors, including perimeter and fence mounted systems and closed circuit television (CCTV) cameras

a. Category I and II premises, and all VAs.	S
b. Category III and IV.	O-S
c. Automatic Access Control Systems (AACS)[5].	O-S
d. Combination and other mechanical lock codes, keys (including spares) of security locks protecting NM/ORM or VAs:	
i. Category I, II, NPS and all VAs	S
iv. Category III and IV.	O-S

1.10 Routine operational procedures covering the use of NM/ORM stores

Security procedures for the issue, receipt and control of stock, names of authorised key holders or monitoring arrangements:	
a. Category I, II, III, IV and all NPS.	O-S

1.11 Security Fences

a. The route of fence lines around or within the site.	Not SNI
b. Details of the construction of a fence and associated physical security features in a given location.	O-S

SECTION 2. OTHER INFORMATION RELATING TO NUCLEAR AND OTHER RADIOACTIVE MATERIAL (NM/ORM) IN USE OR STORAGE

2.1 Quantity, form and source of NM/ORM in use and storage

a. Information about quantity and form of NM/ORM received or held but only if a specific location, (e.g. building number), relating solely to the civil nuclear programme, is shown:	
i. Category I, II and III.	O-S
ii. Category IV.	Not SNI
b. Information about quantity, quality, form or source of nuclear material; supplied to, received by or held on behalf of; or which results from the defence programme[6].	[6]

[5] Any details which could lead to an AACS being defeated or access details to be altered, should be classified appropriately. (see also Section7).

2.2 Waste streams and waste intended for disposal

a. Information relating to radioactive waste streams but only if it enables a specific location (e.g. building number) and the material held there to be identified.

i. Category I, II and III. O-S

ii. Category IV. Not SNI

b. Information held on the BRIMS database(s) or any successor system, unless reported in such a way as to fall within sub para 2.2 c. below or relating to the inventory for disposal in a repository. O-S

c. General information about national radioactive waste streams that does not identify specific location, buildings or relay any exploitable information. Not SNI

d. Any information on waste, (quantities, movements), which identifies the defence programme contribution[6]. [6]

2.3 Throughput

a. Nominal capacity, actual throughput and historical data relating to actual throughput of a plant under Safeguards. Not SNI

b. The same information on a plant which reveals data connected with defence programmes[6]. [6]

SECTION 3. TRANSPORT OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL WITHIN A NUCLEAR PREMISES OR BETWEEN ADJACENT NUCLEAR PREMISES

3.1 Movement plans (Security) and Associated Planning information

a. Information linking Category I and II material with date. O-S

b. Information linking Category III & IV material and ORM with date. Not SNI

3.2 High Security Vehicles (HSV)

(The classifications of various aspects applying to HSV's, are detailed at Section 4.6a).

3.3 Civil Nuclear Constabulary (CNC) escorts

(Classification for information relating to escorts provided by the CNC is detailed in Section 5).

[6] To be protected in accordance with the ACO 300 (Joint MOD/ONR Classification Guide) or with a Security Aspects letter detailing the classification to be applied under the terms of a contract.

SECTION 4. TRANSPORT OF NUCLEAR MATERIAL OFF-SITE

4.1 Transport Security Statements (TSS)

a.	That a carrier has Approved Carrier Status.	Not SNI
b.	TSS for a Class A Carrier.	S
c.	TSS for a Class B Carrier.	O-S

4.2 Transport Security Plans (TptSP)

a.	TptSP for Category I and II.	S
b.	TptSP for Category III.	O-S

4.3 Movement information (Planning)

a.	Category I and II[7].	
	i. Any movement information linking material with date of move.	S
	ii. Information using ONR (CNS) date codes.	O-S
b.	Category III.	O-S
c.	Date codes issued by ONR (CNS) whilst extant.	S

4.4 Notifications[8]

a.	Category I and II (not using date codes).	S
b.	Category I and II (using date codes).	O-S
c.	Category III	O-S
d.	Advance notifications to Euratom (prefixed EURA):	
	i. Category I and II (linking material with date, without using ONR date codes).	S
	ii. Category I and II (separating material and date, without using ONR date codes)	O-S
	iii. Category I and II (Using ONR date codes)	O-S
	iv. Category III and IV	O-S

4.5 Incident reports

a.	Incidents during the transportation of Category I or II nuclear material:	
	i. Initial report.	O-S

[7] Details of material transmitted separately from details of timings and linked only by reference may be transmitted as O-S.

[8] It is recognised that a number of official bodies, including shipping agents, may require movement information, especially in the case of exports of NM; in these cases the bodies will have a *need to know*. Only the minimum information required is to be passed to these bodies and no earlier than necessary.

ii. Full report including assessment of incident.	O-S
b. Incidents during the transportation of Category III nuclear material:	
i. Initial report.	O-S
ii. Full report including assessment of incident.	O-S

4.6 Transport of nuclear material by road

a. High Security Vehicles (HSV):	
i. Visual access to interior of cab or load compartment.	O-S
ii. Physical security features of vehicle design and construction.	S
iii. Design and function of alarms and immobilisation devices.	S
iv. Keys, key designs, combination settings and security locks.	S
v. Frequencies of radio equipment installed on HSV.	O-S
vi. Performance, communications and vulnerabilities of vehicle tracking systems or procedures.	O-S
b. Vehicles transporting Category III nuclear material:	
i. Visual access to interior of cab.	Not SNI
ii. Keys to cab or load compartment when carrying nuclear material.	O-S
iii. Performance, communications and vulnerabilities of vehicle tracking systems or procedures.	O-S

4.7 Transport of nuclear material by rail (General)

a. Keys to locks on a locomotive.	Not SNI
b. Performance, communications and vulnerabilities of vehicle tracking systems or procedures.	O-S
c. Rail wagons for Category I or II movements:	
i. Design and function of alarms and immobilisation devices.	S
ii. Designs and operating systems of security devices securing flasks or containers to/in wagons.	S
iii. Design and construction of internal security arrangements in closed wagons.	S
iv. Keys and combination settings for security locks.	S

4.8 Transport of nuclear material by sea (Category I and II only)

a. Information on ship secure communications systems including types and frequencies, locations of antennae and transmission timings.	S
b. Location and operation of duress alarms.	S
c. Location of Vessel Alarm Station (VAS).	O-S
d. Detailed design, construction and/or capabilities of the VAS.	S

e. Location and function of ship's alarm and back-up systems.	S
f. Overall security arrangements for the vessel including the protection of cargo holds, the bridge, alarms/CCTV control and backup systems.	S
g. Cargo hold access control systems and procedures.	S
h. Location of alarm sensors, surveillance equipment and controlled access doors.	S

4.9 Transhipment points

a. Security plan:	
i. Category I and II.	S
ii. Category III.	O-S
b. Security staffing:	
i. Category I and II (see Section 5.2).	
ii. Category III.	O-S

4.10 Temporary storage during transport

a. Location:	
i. Category I and II.	S
ii. Category III.	O-S
b. Duration:	
i. Category I and II.	O-S
ii. Category III.	O-S
c. Security Plan:	
i. Category I and II.	S
ii. Category III.	O-S

4.11 Nuclear material transport containers

a. Specifications and detailed design data.	Not SNI
b. Methods used to secure flasks to transport.	Not SNI
c. Studies indicating vulnerability of containers to explosives or other terrorist attack methods**.**	S

4.12 Civil Nuclear Constabulary escorts

(Guidance on the classification for information relating to escorts provided by the CNC is detailed in Section 5).

SECTION 5. CIVIL NUCLEAR CONSTABULARY (CNC)

5.1 Information about the strength and deployment of the Constabulary

a.	Overall CNC establishment/strength.	Not SNI
b.	The number of CNC officers established at a site.	O-S
c.	The number of CNC officers on any shift.	O-S
d.	The number of Authorised Firearms Officers (AFO) at a site.	O-S
e.	The number of AFOs on each shift.	O-S
f.	The armed response capabilities and timings at a site.	S
g.	Details of CNC firearms holdings and armouries.	O-S

5.2 Escorts for nuclear material movements

a.	Authorised routes (Route Cards).	O-S
b.	The fact that a movement will be escorted	Not SNI
c.	The fact that the escort will be armed.	Not SNI
d.	The number of officers escorting a movement.	S
e.	Armed response capabilities and timings.	S
f.	Tactical Plans and Operation Orders.	S
g.	Maritime escort specific:	
i.	Location of Vessel Alarm Station (VAS).	O-S
ii.	Function of Vessel Alarm Station (VAS).	S
iii.	Staffing of VAS.	S
iv.	Watch patterns.	S
h.	CNC/Security arrangements at transhipment points.	S

SECTION 6. NUCLEAR MATERIAL ACCOUNTING

6.1 General

a. Statements of general material accounting principles.	Not SNI
b. Description and location of Material Balance Areas (MBA) and of Key Measurements Points (KMP) not already in the public domain.	O-S
c. Physical and chemical form of material measured at those KMP's.	O-S

6.2 Measurements, instrumentation etc.

a. Measurement and instrumentation data which reveal the sensitivity of the measurement system or the alarm limits for Nuclear Material Balance in operation at a particular plant.	O-S
b. Precision and accuracy of standard laboratory techniques[9].	Not SNI

6.3 Nuclear material flow/inventory data

a. Nuclear material flow and inventory information held on IT systems or in hard copy.	O-S
b. Inventory information in other records, if locations are referred to only by code numbers and the key to the code is marked O-S.	Not SNI
c. Euratom Inventory Change Reports, Material Balance Reports and Physical Inventory Listings[10].	Eura R

6.4 Ownership of material

a. Information which reveals any connection with defence matters other than the fact that the materials is 'defence material'[11].	O-S or higher

6.5 Nuclear Material Balance

a. Aggregated annual Nuclear Material Balance figures for a premises which do not reveal the MBA concerned.	Not SNI
b. Nuclear Material Balance in MBAs	O-S
c. Details of investigations into a particular Nuclear Material Balance, unless formally approved for release by the Department of Energy and Climate Change.	O-S
d. Limit of Error for Nuclear Material Balance.	O-S

[9] Some precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could assist terrorists or other would-be diverters. In case of doubt refer to ONR (CNS) (Cyber Security and Information Assurance Team).

[10] For marking of information on advance notifications of movements see Section 4.

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

SECTION 7. COMPUTER SYSTEMS[12]

7.1 Computer Systems Important to Security (CSISy).

a. Computer systems which perform AACS functions for entry to or exit from a nuclear premises or for facilities within a nuclear premises.	O-S or higher
b. Computerised security management systems controlling CCTV and or IDS at a nuclear premises.	O-S or higher

7.2 Computer Based Systems Important to Safety (CBSIS)

a. CBSIS (as identified by ONR safety inspectors or site safety management) on a nuclear premises.	O-S or higher

7.3 Classified Data Networks

a. Reports of security inspections or testing that reveal vulnerabilities	O-S or higher
b. Detailed network diagrams that includes the IP addresses of network switches, devices, etc[13].	O-S or higher[14]
c. Firewall rule sets.	O-S or higher[15]

[12] 'Computer Systems'. (or Information Systems) can include: physical environment (e.g. buildings, communications facilities and links, computer hardware);information and data; software; service provision; people; intangibles (e.g. reputation, goodwill).

[13] Mention of a single IP address or a single device may be not SNI.

[14] Should be classified at the highest level of the information that resides on that network.

[15] Should be classified at the highest level of the information that the firewall(s) is protecting.