Office for Nuclear Regulation

FINDING A BALANCE

(Version 3)

GUIDANCE ON THE SENSITIVITY OF NUCLEAR AND RELATED INFORMATION AND ITS DISCLOSURE

Office for Nuclear Regulation

2nd April 2014

This page is intentionally blank

CONTENTS

PREFACE

There are many official sources of information about civil nuclear materials and facilities. Following the terrorist acts in New York and Washington on 11 September 2001, concern was expressed in various quarters about the amount of information that was so publicly and easily available to terrorists. There was increased awareness that the ease with which such information could be obtained made it easier for terrorists and others to make their plans without taking any risks. It was recognised that the benefits of a culture of openness were accompanied by risks.

There is a considerable body of legislation that requires disclosure of information for a variety of purposes. Some of these are official purposes to do with planning, environmental protection etc. Others are to do with public information and consent. The purpose of this document is to assist officials and others involved with the civil nuclear industry to manage the risks associated with compliance with their legal obligations. It is not intended in any way to water down those legal obligations only to help, if possible, lessen the ease with which those with malevolent intent can obtain the information they need.

In support of the Government's desire for transparency, this Guide carries no protective marking. It may seem paradoxical to identify publicly the types of information that could be used by terrorists. But the balance of advantage is in increasing awareness. In any case, there is nothing sensitive about, for example, stating that information about the quantities and whereabouts of plutonium is sensitive. It is the actual information that is sensitive. It may not be possible to protect the information totally but the purpose of this Guide is to help readers think about it. Is it, for example, necessary on all plans to identify a plutonium store or only on those plans used by those with an operational reason for knowing? And is it possible for these plans to be labelled as sensitive and given some protection? The answers may be negative but the issue requires thought.

A considerable amount of such information is already easily available. There is no way of recalling it. Details do, however, change. Often they change over quite short periods of time. Published information becomes unreliable if it is not regularly updated. One purpose of this guide is to begin that process. The guide, although published by the Office for Nuclear Regulation as part of its remit, has been produced after widespread consultation with the industry, government departments and agencies, and the devolved administrations. It must be understood that this document provides guidance only. It is not a statutory instrument and has no force in law. However, further guidance should be sought from the appropriate department/authorities if a statutory requirement to release information seems at variance with this guide.

No document of this nature can be completely definitive and cases may arise where it provides little or no help. It is intended to be a dynamic document and may be amended through experience. As with any information covered by the FOI Acts and other Regulations, a decision not to disclose that is based on this guide may be open to challenge. Any such challenge will be dealt with on a case-by-case basis. ONR believes, however, that a decision not to disclose that draws on the sensible use of this guide is more likely to be upheld.

The Ministry of Defence has a number of Guides concerning the protection of information related to the security of material used in the nuclear weapon and nuclear propulsion programmes. These programmes are outside the scope of this Guide.

This version of the guidance (version 3) was revised to incorporate the new UK Government Security Classification (GSC) scheme that was introduced on 2nd April 2014.

This page is intentionally blank

PART 1

WHAT IS THE PROBLEM?

If nuclear material were to be stolen or sabotaged, for example by terrorists, the potential consequences could be extremely grave. Nuclear material, its transport, and the processes in which it is used for civil purposes - principally power generation - need to be well protected. In the United Kingdom, a high level of security is expected at nuclear sites and there is a strict process of regulatory enforcement by the Office for Nuclear Regulation. An important aspect of this security is the protection of information about civil nuclear material and operations and, of course, information about security measures. However, such knowledge and information is also a necessary, often essential, part of running the business. Some information may need to be available to a large number of people. Not all of these are part of the industry e.g. planners, police etc. Members of the public may also have a legitimate interest in information about nuclear facilities and operations.

The problem is how to reconcile these apparently conflicting requirements. How can information be made available to those who need it whilst keeping it from those who could take advantage of it for their own malign ends?

Few would advocate total openness of all nuclear related information. But if some knowledge is to be restricted, how do you decide what that is, to whom it should be restricted, and how do you ensure that they are able to keep it secure? Not all organisations need high levels of security for the rest of their business. When a large number of people need to know something in order to carry out their job, the knowledge is hardly a secret even though it could be misused. Neither total openness nor total security are viable options.

WHAT CAN BE DONE?

Some of the obligations about disclosure are described in Annex A. In a situation of conflicting demands and interests, a single overriding solution is unlikely to be available. In any case, situations rarely remain static. Information that is not required one day, may be required the next. Case -by-case judgments are often required. Are the risks of not disclosing something greater or less than the harm occasioned by disclosing it? Knowing why to disclose something is usually easy. But there may be little or no awareness of why it might not be such a good idea. What is needed is information about disclosure that could have adverse consequences. With that information, an informed judgment on the risks can be made. If there are risks in disclosure:

-is it in the public interest to provide access to the information?
-should it be provided only to those who can secure it?
-can the information be edited so it is less sensitive but still useful?

WHAT IS THIS GUIDE FOR?

This document describes the types of information which could be useful to terrorists and others of malign intent. It is intended as a guide, particularly to those unfamiliar with such matters, to the risks and dangers associated with automatic disclosure. It is intended to assist users in deciding whether information should be formally secured and whether to seek alternative means of achieving the same purpose.

WHAT THIS GUIDE IS NOT!

This is a guidance document. No obligations are implied by it and, importantly, it should not be regarded as contradicting any of the wide variety of legislation that requires certain types of information to be shared or made public. Its aim is to assist readers to be aware of, and where possible to minimise, the risks associated with those obligations.

PART 2

HOW TO USE THIS GUIDE

There should be a presumption of openness unless there are cogent and defensible reasons against it. The defensible reasons need to fit within the meaning of one of the exemptions in the Freedom of Information Act 2000. This Guide has been compiled in tabular form (Part 3) to inform decisions about which information, because of its potential value to terrorists or others with malevolent intent, should not be disclosed. It should, for example, be of assistance to those compiling safety cases and planning applications. Such documents often contain sensitive information about a nuclear facility. This Guide may assist in identifying to the safety and local government authorities those parts of the documents which they should protect and not make available to the public.

This Guide is concerned with the sensitivity of information, including that held on computer systems, relating to Nuclear Material (NM), Other Radioactive Material (ORM) and facilities housing such material. The special objective of this Guide is to prevent the disclosure of information that could assist a person or group planning theft, blackmail, sabotage and other malevolent or illegal acts. Its application is an integral part of the protection of data on NM/ORM and the facilities housing such material. These data fall into the following categories:

- information on the physical security arrangements in place to protect NM/ORM and the facilities;
- technical guidance on security standards and requirements;
- information on the quantity and type of material at a facility and its location;
- inventories, throughput, output, storage capacity of facilities and accounting;
- detail of planned movements of NM/ORM;
- technical information about the production or processing of NM;
- information contained in facility IT systems;
- information on computer systems important to security and to safety;
- information contained in safety cases and other documents which describe facilities;
- information contained in planning applications;
- information about the deployment and operations of the Civil Nuclear Constabulary (CNC).

Official disclosure of information concerning NM/ORM and the facilities that contain such material should be considered only after this Guide has been consulted. The policy is not designed to protect commercial information, although it is recognised that, occasionally, some commercial information may contain sensitive data. Unless it conflicts with this Guide the release of such information would be at the discretion of local management.

Effective use of this Guide requires some understanding of the Government Security Classification (GSC) system used by government and the categorisation of NM/ORM.

- The GSC system is a way of indicating that information should be seen only on a need-to-know basis and that it should receive appropriate protection. It is based on the damage that could arise if the information were to be seen outside of the need-to-know group. It is not usual to attach visible labels to physical assets but the same principles can be applied. The explanations used in this Guide for not releasing information are also those that would be used to determine the appropriate Security Classification. It is convenient, therefore, to indicate the sensitivity of particular sorts of information through the use of the national system

of Security Classifications as this is also indicative of the security levels that are required. The definitions of the Government Security Classifications are given in Annex B.

- NM, including nuclear waste depending on its nature, are placed into one of four categories, denoted by the characters I to IV. The importance of the material and, therefore, the protection applied to counter theft or sabotage is determined by the Category into which it falls; material in Category I requires a greater level of protection that that in Category IV. Nuclear licensed sites are also given a similar category dependent upon the material that is stored or processed there. The UK Categorisation Table is reproduced at Annex C.

PART 3

3.1 GUIDANCE TABLES

The tables in this Part provide detailed guidance to inform decisions about information that should not be released and the reasons why not. In some instances the reason for non-disclosure cites exemption given by sections of the Freedom of Information Act 2000 (a cross reference to the Freedom of Information (Scotland) Act 2002 is provided in Annex A). It should be understood that a malevolent act on a nuclear facility may give rise to a release of radioactivity which may be confined to the site or, worse, may affect an area surrounding the site. Information which, if disclosed, could lead to an action which could cause such a release of radioactivity would be exempt under section 38(1) of the FOI. Such information, depending on circumstances, could also be exempt under section 31(1)(g) and subsections (2)(i) and (j). Sensitive information may also be exempt under section 24(1), National Security. The term was defined by John Major, the then Prime Minister, in the House of Commons in June 1992 as "….the safeguarding of the state and community against threats to their survival or well being". These sections of the Act are implicit and, therefore not quoted in the tables. Also implicit are the provisions of regulation 12(5)(a) of the Environmental Information Regulations 2004, which provides for exception of information, the disclosure of which would affect, inter-alia, public security.

Topic	Sensitivity	Reason for Protecting
0100 Security of Nuclear Material and Facilities		
0101 Regulations and Guidance		
a. Nuclear Industries Security Regulations (NISR) 2003	Releasable	None
b. Guidance to NISR 2003	Releasable	
c. NORMS for NISR 2003	Not Releasable	This document contains details of standards, types of equipment to be used, procedures and security operations details of which would be of great use to a person or group planning to attack a nuclear facility for the purposes of theft or sabotage. (the information contained in the document has the protective marking SECURITY CLASSIFICATION of (OFFICIAL-SENSITIVE)

Topic	Sensitivity	Reason for Protecting
0102 Security Plans for Licensed Nuclear Sites All sites	Not Releasable	Security plans contain detailed descriptions of the security regime in place at a site and precise detail of where within the site nuclear material is stored and details of other areas vital to the site. Such information would be of great value to any person or group planning to attack a nuclear facility for the purpose of theft or sabotage. (Security plans for Category I to III sites would have a SECURITY CLASSIFICATION of SECRET. Those for Category IV sites have a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0103 Security Reports a. Reports from security surveys, inspections and assessments and other reports on the physical security or technical security measures employed on a nuclear site.	Not Releasable	Access to these reports can provide persons with malevolent intent with detail on the location of nuclear materials, the measures taken to protect them and any assessed vulnerabilities there may be; thus assisting them to avoid security measures and controls. (Security Reports will attract a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
b. Reports describing critical features and/or highlighting requirements for security improvements for: • Category I, II and III nuclear material • Category IV nuclear material • Vital Areas	All below Not Releasable	Information of this nature will be of great assistance to persons wishing avoid security arrangements and assist with targeting a nuclear facility. (These reports merit a SECURITY CLASSIFICATION of SECRET) (These reports merit a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE) (These reports merit a SECURITY CLASSIFICATION of SECRET)
c. Results of security investigations at a nuclear site, including those into leaks of sensitive information	Not Releasable	Exempt information under FOI, section31(g) and subsections (2)(b) or (i) or (j)
0104 Details of construction and layout of		Official maps, chart or plans of sites

Topic	Sensitivity	Reason for Protecting
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 at: a. Category I & II b. Vital Areas and NPS c. Category III d. Category IV	All Not Releasable	may be released at the discretion of site management, provided they contain no description of the details of a building's functions, the materials stored therein and the location of internal security fences and the other security measures employed at the building. Knowledge of this nature can assist persons to avoid security arrangements and possibly assist with targeting. (This information would be classified as OFFICIAL-SENSITIVE to SECRET dependent on the level of detail included)
0105 The types and locations of intruder detection system (IDS) sensors and the associated CCTV cameras, including circuit diagrams and cable runs, and the maintenance and testing programmes for these equipments	Not Releasable	Any details which could assist in the security systems at nuclear facilities being defeated by an attacker must be protected. FOI section 31(1)(a) may apply. (This information merits a SECURITY CLASSIFICATION of SECRET for Categories I and II and OFFICIAL-SENSITIVE for Categories III and IV)
0106 Details of Automatic Access Control Systems (AACS), including the location of computer servers and back-up servers.	Not Releasable	Any details that could lead to the AACS system being defeated by an attacker, insider or outsider, should not be released. (Such information requires a SECURITY CLASSIFICATION of SECRET for Categories I, II and Vital Areas and OFFICIAL-SENSITIVE for Categories III and IV)
0107 Stores: security procedures for the issue, receipt and control of stock; names of authorised key holders; arrangements for monitoring and guarding:	Not Releasable	Of great potential assistance to attackers (whether they be insiders or outsiders) who may be considering sabotage or theft of nuclear material. (Information of this attracts a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0108 General maps showing the position and limits of a nuclear facility but without detail of what is contained therein	Releasable	None The Nuclear Installations Act 1965 requires the Minister to maintain a

Topic	Sensitivity	Reason for Protecting
		list of licensed sites and maps showing position and limits and to ensure the list is available to the public. This information does NOT attract a protective marking.
0200 Information Relating to the Quantity and Form of Nuclear Material		
0201 Information about the quantity and form of nuclear material received or held in specified locations relating solely to civil nuclear programmes:		Information of the sort contained in this section could be an aid to choosing targets while planning attacks.
a. Category I, II and III	Not Releasable	(Information normally attract a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
c. Category IV	Releasable	None
0202 Throughput – nominal capacity, actual throughput and historical data on throughput of a plant under Safeguards	Releasable	None
0300 Nuclear Material in Transit (Including Movements within Sites)		
0301 Information on Category I - III movements with date.	Not Releasable	Information of this sort would be an aid to choosing targets while planning attacks for theft or sabotage on material in transit. (information normally attracts a SECURITY CLASSIFICATION of SECRET)
0302 Information on Category IV movements with date.	Releasable with discretion	Information of this sort could be an aid in planning theft or sabotage attacks so information should be treated with care (does NOT normally attract a security classification
0303 High Security Vehicles (HSV)		
a. Visual access to interior of cab and cargo compartment	Not Releasable	HSV carry fissile material and any information of the type listed in this section would be of use to an attacker planning an attempt to steal or sabotage fissile material in transit.
b. Physical security features of vehicle design and construction	Not Releasable	

Topic	Sensitivity	Reason for Protecting
c. Design and function of alarms, immobilisation devices and key designs for special locks d. Load compartment keys, spare keys and combination lock settings, where used	Not Releasable Not Releasable	(The appropriate SECURITY CLASSIFICATION for the various aspects opposite would be: a. OFFICIAL-SENSITIVE b, c and d. SECRET)
0304 Vehicle tracking system; performance and communications	Not Releasable	HSV carry fissile material and any information of the type listed in this section would be of use to an attacker planning an attempt steal or sabotage fissile material in transit. (Detail of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
0305 Nuclear Material Transit Containers: a. Level of resistance of transport containers of containers to attack by various means b. Specifications and design data on containers	 Not Releasable Releasable	 Useful to an attacker planning a sabotage attack with the aim of releasing radioactive material, or theft of the material. (The data at a, would attract a SECURITY CLASSIFICATION of SECRET)
0400 IT Systems & Computer Systems Important to Security and Safety		
0401 Details of IT Systems storing and processing OFFICIAL-SENSITIVE information, the architecture of the systems and details of security measures employed and where back-up data is stored	Not Releasable	Useful information for a person or group planning theft, sabotage or other malevolent act at a nuclear facility. (Details of such systems would require a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0402 Details of computer systems which perform access control for entry to and egress from a licensed nuclear site and to other facilities within the site and other security functions; and information on the location of back-up hardware and software	Not Releasable	Information useful to a person or group planning theft, sabotage or other malevolent act at a nuclear facility. (Detail of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
0403 Fact that systems controlling access may also have a safety mustering function	Releasable	

Topic	Sensitivity	Reason for Protecting
0404 Details of computer based systems important to safety installed on licensed nuclear sites, as Identified by ONR safety inspectors or site safety management	Not Releasable	Compromise of these systems could permit an attacker to at least disrupt the operations of a facility. In the worst case disruption could lead to a radioactive release. (Detail of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE or higher)
0500 Civil Nuclear Constabulary (CNC)		
0501 The Civil Nuclear Police Authority		
a. Composition and appointments	Releasable	
b. Periodic general reports	Releasable	
0502 The Constabulary		
a. Overall establishment and the current strength of the force	Releasable	Available in Chief Constables Annual Report
b. Establishment and current strength at particular sites	Not Releasable	Information of this nature would be very useful to any individual or group in planning an incursion into a nuclear site for the purpose of sabotage or theft and would seriously undermine the capability for effective response to an attack. (Detail of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
c. Numbers on any shift at a site	Not Releasable	(Details of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
d. Number of authorised firearms officers at individual sites	Not Releasable	Any information that would help a terrorist group to estimate in advance the scale of response and the capabilities available in a CNC operational unit must be protected from disclosure. (Details of this nature would require a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
e. Armed response capabilities and timings at a site	Not Releasable	(Details of such systems would require a SECURITY CLASSIFICATION of SECRET)

Topic	Sensitivity	Reason for Protecting
0503 CNC escorts for movements: a. That escorting CNC officers may be armed	Releasable	
b. Deployment and strength of escorts	Not Releasable	Information of the nature contained in sub-paragraphs b and c would be of great use to an individual or group planning to attack a convoy
c. Radio frequencies in use to enable communication with County or Regional Police Forces	Not Releasable	(Details of this nature would require a SECURITY CLASSIFICATION of SECRET)
0600 Nuclear Material Accounting		
0601 Description a. Statements of general material accounting principles	Releasable	
b. Description and location of Material Balance Areas (MBA) and Key Measurement Points (KMP) not already in the public domain	Not Releasable	Reveals details of location and quantities of fissile material that would be of use to an attacker planning theft of nuclear material or sabotage.
c. Physical and chemical form of material measurement at KMP	Not Releasable	(Details of this nature would attract a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0602 Measurements and instrumentation data: a. Data which reveals the sensitivity of measurement or the alarm limits for Nuclear Material Balance at a particular plant	Not Releasable	
b. Precision and accuracy of standard laboratory techniques	Releasable	Some precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could assist terrorists or others planning theft of material (Details of this nature require a

Topic	Sensitivity	Reason for Protecting
		SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0603 Nuclear material flow and inventory data a. Nuclear material flow and inventory data held on IT systems, in hard copy or on any form of storage medium.	Not Releasable	Information of this nature could reveal exact details of the location and movements of nuclear materials
b. Inventory information in other records, if locations are referred to by code numbers and the key to the code is marked OFFICIAL-SENSITIVE	Not Releasable	(Details of this nature would require a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
0604 Nuclear Materials Balance (NMB) a. Annual NMB figures for a site which do not reveal the MBA concerned b. NMB in MBAs or KMPs d. Details of investigations into particular NMB unless formally approved for release e. Limit of Error for NMB (LENMB) or other specific indications of the uncertainty of NMB figures	Releasable Not Releasable Not Releasable Not Releasable	Following DECC's formal approval the companies in the civil nuclear industry publish annually an overall NMB figure for each of their sites for safeguarded plutonium, high enriched, low enriched, natural and depleted uranium. Provided that protectively marked or commercial information is not disclosed, questions arising from the publication of NMB figures can be answered. It is not intended that NMB data should be withheld solely on the grounds that it would cause embarrassment to the companies (Details of this nature may attract a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE or higher)
0700 Planning Applications		
0701 Planning applications should contain only the minimum information required by law: a. Plans and drawings should contain only the detail necessary and must not indicate location of security equipment b. Detailed description of the function of the building is to be avoided although building numbers may be used	Releasable (with discretion)	If it becomes necessary to provide the planning authority with more than the basic information, this information should be contained in an annex and protectively marked appropriately. The planning authorities should be notified that is to be protected and is not for public consumption. Attention of the planners should be drawn to Section 79 of the Anti-Terrorism, Crime and Security Act 2001.

Topic	Sensitivity	Reason for Protecting
c. Fence lines may be indicated but detail of the fence structure should be avoided		Operators should consult the appropriate local authorities and apprise them of the sensitivity of any information in the application which requires protection and that it should not be available for public scrutiny (some information that is attached to an application may attract a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
0800 Safety Cases and Other Safety or Environmental Information		
0801 Safety Cases a. Safety cases of all classes		
• details of the potential hazards or other information that could be used as a surrogate for evaluating the impact of a release, or details on the impacts of releases;	Not Releasable	The type of detailed information contained in safety cases would be of great use as an aid to a potential attacker for choosing targets and planning an operation.
• details of strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure material;	Not Releasable	
• details of essential services which underpin systems and structures designed to contain, control or secure material;	Not Releasable	
• details of access to the production process, both physical access control and removal of material from the process for control and monitoring purposes. (note: any safety case which contains information included elsewhere in this Guide must take account of the sensitivity of that information)	Not Releasable	(all of the information detailed in the bulleted list attracts a SECURITY CLASSIFICATION of at least OFFICIAL-SENSITIVE)
b. Safety case summaries	Releasable	For Safety Category (SC) 3 there may be no summary; the SC3 Log will substitute

Topic	Sensitivity	Reason for Protecting
0900 Contingency and Emergency Plans & Exercises		
0901 Contingency and emergency plans Existence of and details in Contingency and Emergency plans for a radiological incident at a facility	Releasable	
0902 Security Contingency Plans Detail in security contingency plans for a nuclear facility	Not Releasable	Such plans contain detailed information on the security regimes and procedures in place. They would also contain information on the capabilities of the police or guard force contingents and on the likely response to a security incident. All would be very useful to a would-be attacker. FOI section 31(1)(a) may apply. (Details of this nature would require a security classification of at least OFFICIAL-SENSITIVE)
0903 Exercises a. That an exercise is to take, or has taken place	Releasable	
b. Details of security exercises at a facility	Not Releasable	Provides would-be attackers with information concerning nature and timing of response, detail of armed response force, nature of tactics employed and signal plan (Depending on the nature of the exercise, a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE or higher may apply)
c. Details of safety exercises	Releasable (with discretion)	Information concerning the location and contents of buildings at a facility of particular sensitivity should not, however, be released, as it would provide a potential attacker with useful planning information

Topic	Sensitivity	Reason for Protecting
1000 Personal Information		
1001 Personal information		
a. Information in vetting files	Not Releasable	Information of this nature could be used by a potential attacker to attempt to suborn or otherwise exert pressure on an individual working at a facility or on an individual associated with a facility.
b. Information in personal files	Not Releasable	(Protection for this type of information is afforded by vetting confidentiality and by the Data Protection Act. It would normally be covered by the SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE PERSONAL) See also s40 of FOI
1100 Radioactive Waste Inventory		
1101 Information on radioactive waste streams:		
a. General information that does not identify a building or location and does not contain any other information that would be exploitable	Releasable	
b. Information that enables a specific building at a facility and the material held there to be identified	Not Releasable	Provides targeting information for an attacker planning sabotage (Details of this nature would require a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
1102 The BRIMS database, which contains very detailed Radwaste information supplied by operators. (Note: some specific information is extracted from the database to prepare Defra's national inventory of waste)	Not Releasable	(Details of this nature would require a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)

Topic	Sensitivity	Reason for Protecting
1200 Decommissioning		
1201 Plans to decommission plant, provided detail of precise quantities and locations of nuclear material or waste are not revealed. (included in the above are the following types of document:	Releasable	
a. Life-cycle Baselines (LCBL) b. Near Term Work Plans (NTWP) c. Article 37 Submissions (required by EURATOM Treaty)	Releasable after review	To ensure no sensitive information is inadvertently released, documents of this nature must be subject to a security review before release into the public domain. Where there is doubt, ONR CNS should be consulted.
1202 Waste from decommissioning		
a. That a store is to be built and location	Releasable	
b. Detail of the construction, security measures and quantity of material to be stored in new builds for the treatment and storage of waste and arisings	Not Releasable	Provides good targeting information for an attacker planning sabotage attacks. (Details of this nature would require a SECURITY CLASSIFICATION of OFFICIAL-SENSITIVE)
c. Details in contracts concerning security of waste streams, routes, storage	Not Releasable	Would provide advance targeting information to a person or group intending to attack a facility.
d. Details of quantity, type and location of waste and arisings stored	Not Releasable	(could attract a SECURITY CLASSIFICATION of up to OFFICIAL-SENSITIVE)
1300 Historical Information		
1301 Historical information, not already in the public domain, that contains information currently relevant and still sensitive (in relation to the other sections in this document), whether or not a protective marking has been applied.	Not Releasable	Information of this nature, although old, may still be of use to malevolent persons planning action against a facility. (Could be security classified up to and including SECRET) Operators should review their historical data to ascertain what might fall into this category

Topic	Sensitivity	Reason for Protecting
1400 Threat Assessments and Security Alerting Information		
1401 Annual threat assessments issued by JTAC/DECC/ONR (CNS)	Not Releasable	Exempt under FOI section 23(1) (Security Classified up to and including SECRET)
1402 Design Basis Threat renamed The Nuclear Industry Malicious Capability Planning Assumptions	Not Releasable	Exempt under FOI section23(1) (Security Classified up to and including SECRET)
1403 Reasons for current Response Level in place and for changes in Response Levels	Not Releasable	Exempt under FOI section 23(1) (Security Classified up to and including SECRET)

Annex A

LEGISLATION ON DISCLOSURE

The access provisions of the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 come into force on 1 January 2005 and create a statutory right of access to information held by a Public Authority and provide a scheme for making information available. The Acts cover a wide range of public authorities and include public companies (see section 6 and Schedule 1); included are central government, local government, NHS bodies, schools, colleges, the police; other public bodies and offices. The former UKAEA is a public authority under Schedule 1 Part VI and former BNFL another, under section 6 of both the FOI Acts. Section 6 does not appear to apply to other companies in the civil nuclear industry, although each should review its position there under. Section 4(1) of both Acts, however, provides that the Secretary of State (or Scottish Minister) may, if certain conditions are met, add to the schedule. The Nuclear Decommissioning Authority (NDA) is one such addition.

Regulated by a Commissioner to whom the public have direct access, the FOI Act permits people to apply for access to information only. Whilst providing such right of access, the Acts also create exemptions from the duty to disclose and establishes the arrangements for enforcement and appeal. The Act also requires public authorities to inform the individual who requested it the basis for refusing a request for information, which must be made on the basis of the exemptions in the Acts.

Information may be withheld legitimately under the FOI Acts where an exemption applies or a public interest test is satisfied. Simply because information attracts a protective marking does not mean that it cannot be disclosed. In reality, however, if information has been protectively marked appropriately it is highly likely that the ‘public interest’ considerations that the Acts require have been taken into account and that the information may be withheld.

Environmental legislation provides for the placing of information relating to activities under various regulatory regimes on public registers. In most cases the Secretary of State has the power to direct that information should be withheld on the grounds of national security. In addition, the Environmental Information Regulations 2004 require the provision of “environmental information” by certain public bodies upon request. This requirement is subject to certain exceptions, notably where disclosure would affect international relations, national defence or public security.

FREEDOM OF INFORMATION ACTS

Part 2 of both the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 detail information that is exempt from disclosure, without being subject to a public interest test. The relevant Sections in each Act are, however, not always the same. When in this document there is a reference to a Section of the Freedom of Information Act the reference is from the FOI Act 2000. The comparison table and notes below enable cross-reference between the two Acts.

Aspect	FOI Act 2000 Section No	Scottish Act 2002 Section No
National Security	24	Both 31
Defence	26	
International Relations	27	32
Economy	29	Both 33
Commercial interests	43	
Public authority investigations	30	34
Law enforcement	31	35
Effective conduct of public affairs	36	30
Health and Safety	38	Both 39
Environmental	39	
Personal information	40	38
Information provided in confidence	42	36
Disclosure of environmental information	74	62
Removing restrictions on disclosure	75	64

General Points

Where the FOI Act 2000 defines exempt information as that which “would, or would be likely to, prejudice”, the Scottish Act states “prejudice substantially”.

The FOI Act 2000 has “The duty to confirm or deny does not arise if, or extent to which compliance with section …..”. The Scottish Act does not have this provision.

In the Scottish Act “Scottish Ministers” replaces the “Secretary of State” throughout.

National Security and Defence

Whereas the FOI Act 2000 requires a Minister of the Crown to certify information is exempt, the Scottish Act requires a Member of the Scottish Executive to do so.

Public Authority Investigations/Law Enforcement

The differences between these sections in the FOI Act 2000 and in the Scottish Act are to take account of Scottish law and associated terminology.

Effective Conduct of Public Affairs

The FOI Act 2000 has the requirement for judgements to be made “in the reasonable opinion of a qualified person”, the Scottish Act does not contain this provision.

Information Provided in Confidence

S36(1) of the Scottish Act – Information in respect of which a claim to confidentiality of communications could be maintained in legal proceedings is exempt information – this is not reflected in S41 of the FOI Act 2000.

This page is intentionally blank

Annex B

DEFINITIONS OF SECURITY CLASSIFICATIONS (2014)

Definition of OFFICIAL

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the „need to know". In such cases where there is a clear and justifiable requirement to reinforce the „need to know", assets should be conspicuously marked: „'**OFFICIAL–SENSITIVE'**

Definition of SECRET:

Very sensitive HMG (or partner's) information that requires protection against the highly capable threat profile, **AND** where the effect of accidental or deliberate compromise would be likely to result in any of the following:

- Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
- Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:
  i. Current or future capability would be rendered unusable;
  ii. Lives would be lost; or,
  iii. Damage would be caused to installations rendering them unusable.
- Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
- Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.
- Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.
- Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
- Cause major impairment to the ability to investigate or prosecute serious organised crime.

:

This page is intentionally blank

Annex C

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

This page is intentionally blank

Annex D

GLOSSARY

The following abbreviations are used within this document:

AACS	Automatic Access Control System
ATC&S	Anti-terrorism, Crime and Security Act 2001
BRIMS	British Radwaste Information Management System
CCTV	Closed Circuit Television
CNC	Civil Nuclear Constabulary
DCNS	Director of Civil Nuclear Security
ETUK	Enrichment Technology UK Ltd
FOI	Freedom Of Information Act 2000
FOI(S)	Freedom of Information (Scotland) Act 2002
HSV	High Security Vehicles
IAEA	International Atomic Energy Agency
IDS	Intruder Detection System
KMP	Key Measurement Points
LEMUF	Limit of Error for MUF
LMU	Liabilities Management Unit
MBA	Material Balance Area
MOD	Ministry of Defence
MUF	Material Unaccounted For
NDA	Nuclear Decommissioning Authority
NM	Nuclear Material
NPS	Nuclear power stations
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PIDS	Perimeter Intruder Detection System
P-M	Protective Marking
SC	Safety Category
UCL	Urenco (Capenhurst) Ltd