

**HSE Nuclear Directorate
Division 5
Office For Civil Nuclear Security**

**The Management of Sensitive
Nuclear Information during the
Generic Design Assessment of
Nuclear Technologies.**

**Version 2
01 February 2008**

Introduction

The generic design assessment process being introduced by the nuclear regulators for new nuclear technologies involves the submission by requesting parties of written details of these technologies and subsequent interaction with regulators on their content. Although it is the intention that, as far as possible, details of these technologies will be made available to the public, clearly some detail could be of use to terrorists for planning purposes. Such information is known as “sensitive nuclear information”.

The purpose of this guidance note is to draw attention to the need to identify sensitive nuclear information contained in generic design assessment submissions, outline how such information should be initially protected by applicants in accordance with the Nuclear Industries Security Regulations 2003 (NISR) and inform requesting parties how further advice will be provided in due course by the Office for Civil Nuclear Security (OCNS). It is specifically aimed at requesting parties who are not currently holders of a nuclear site licence.

Finding a Balance

There are many official sources of information about civil nuclear materials and facilities. Following the terrorist acts in the US on 11 September 2001, concern was expressed in various quarters about the 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.

As a result, OCNS published a document “Finding a Balance – Guidance on the Sensitivity of Nuclear and Related Information and its Disclosure”. A copy of Issue 2 of this document dated April 2005 is available on the DTi website. The objective of this document is to prevent the disclosure of information that could assist a person or group planning theft, blackmail, sabotage and other malevolent or illegal acts. It identifies categories of information which should not be disclosed, provides reasons for protecting this information and indicates the appropriate protective marking to be afforded to such information.

Nuclear Industries Security Regulations 2003

There are now revised statutory requirements on all persons to protect sensitive nuclear information as a result of amendment of Regulation 22 by the Nuclear Industries Security (Amendment) Regulations 2006. Regulation 22 applies to any person who holds sensitive nuclear information and is proposing to become involved in activities on or in relation to a UK civil licensed nuclear site, in particular for the purposes of planning, designing or constructing any proposed installation on a nuclear site.

Sensitive nuclear information is defined as *“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,” whilst information which needs to be protected in the interests of national security is further defined as including *“information which requires a protective marking in accordance with the classification policy”*. It does not include information which has *“previously been made available to the public anywhere in the world”* otherwise than in contravention of the law.

The classification policy is contained in the document ‘Information Concerning The Use, Storage and Transport of Nuclear and Other Radioactive Material’, issued by OCNS. This document deals with how information should be protectively marked and not with issues concerning disclosure policy. It is concerned with both documents and information held on computer systems. Effective application of this guide is considered an integral element in the security of nuclear material and prevention of the disclosure of information that could assist those planning a terrorist act, theft, sabotage or other malicious acts.

A person subject to Regulation 22 is required to 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, sensitive nuclear information within his possession or control. The principal person in any body holding sensitive nuclear information is further required to ensure that all of his officers, staff, contractors and consultants are familiar with the required security standards, procedures and arrangements for the protection of sensitive nuclear information held by that body.

Disclosure of Nuclear Information

The document ‘Finding A Balance’ provides adequate initial guidance to applicants on the classification policy of nuclear and related information that is likely to be initially submitted by them as part of the Generic design assessment process. Some relevant examples of information, further detailed in the ‘Finding a Balance’ document, that should not be made public are given below:

- Safety Cases that could identify a means of causing a significant radiological release from a plant
- Security Plans and details of security architecture
- Details of construction and plant layouts showing features of physical security relevant to the prevention of theft and sabotage
- Vital Area critical features, including features of physical security (Vital Areas are defined as areas containing nuclear material, equipment, systems or devices, the sabotage of which could directly or indirectly result in serious radiological consequences)
- Details of computer systems important to safety (including the locations, functions and upgrade routes for the systems)
- Details of proposed on-site storage of nuclear material

Process Management

Requesting parties intending to submit design information as part of the pre-licensing process will therefore need to be familiar with the contents of:

- NISR, in particular its 2006 amendment of Regulation 22; and
- The 'Finding a Balance' document

Prior to submitting any design submission, requesting parties will need to identify information which is "not releasable" in accordance with the Finding a Balance document. Where possible, this "not releasable" information should be separated from other information to be submitted but, in any event, it should given a protective marking of at least RESTRICTED. This RESTRICTED information should be marked, protected and transmitted in accordance with the guidance contained at Annex A in order to comply with the provisions of Regulation 22(7)(a).

Should a requesting party consider that information generated as part of the generic design assessment submission should be marked CONFIDENTIAL, then he should follow the guidance given in Annex B.

Following receipt OCNS will examine selected information submitted as part of the generic design assessment process with a view to:

- Confirming that information is correctly marked in accordance with the classification policy; and
- Identifying any other information which should bear a protective marking in accordance with the classification policy

OCNS will communicate the outcome of this protective marking review to the requesting party as soon as possible. In the event that it decides information should bear a CONFIDENTIAL marking, it will inform the requesting party of this requirement. As part of this process, the Secretary of State, through OCNS, will issue a direction to the applicant under Regulation 22(7)(b) requiring him to take specific measures to protect the information concerned in accordance with this policy and these instructions.

In all cases, it is anticipated that as the generic design assessment process proceeds it will involve more detailed exchanges between the requesting party and OCNS on security aspects of the design which will need to be taken into account by the applicant if and when a submission is made for a licence to install the design at a UK site. As these exchanges will involve CONFIDENTIAL and/or possibly SECRET information, OCNS will first take action as outlined above if this action has not already been carried out.

In order that sensitive nuclear information may be properly controlled throughout the generic design assessment process, requesting parties will be required to establish a UK office(s) at which protectively marked information is appropriately protected. Any UK generated sensitive nuclear information

passed to the requesting party or incorporated into the design during the generic design assessment process is not to be transmitted outside the UK without prior approval from OCNS.

Contact

Further advice on this issue may be obtained by potential applicants from the Principal Inspector (Information Security), OCNS, telephone 01235 432959, fax 01235 432926.

ANNEX A

GUIDANCE ON THE PROTECTION AND MANAGEMENT OF RESTRICTED INFORMATION

Introduction

1. Access to RESTRICTED information should be strictly controlled in accordance with the 'need to know' principle. It should be confined to those employees whose access to the information is essential for the purpose of their duties.

Personnel Security

2. Employees and contractors having access to RESTRICTED information should be warned that the Anti-Terrorism, Crime and Security Act 2001 includes provisions prohibiting the disclosure of sensitive information relating to nuclear security. This reflects the importance of safeguarding information from damaging disclosure which could prejudice the security of nuclear sites and nuclear material on sites or being transported anywhere in the world. Such disclosures could assist terrorists or others intending to attack or sabotage nuclear sites or steal nuclear material.

3. Section 79 of the Act makes it an offence to *intentionally* or *recklessly* disclose information which might prejudice the security of a nuclear site and nuclear material, whether on site or being transported, including on board a British ship.

Transmission within Sites or Companies

4. RESTRICTED information should be transmitted within sites and companies in such a way as to ensure that no unauthorised person can have access. RESTRICTED data should not be placed on an IT system or transmitted by an Intranet IT system unless the system has been accredited by OCNS through the Company Security Manager.

Transmission Outside Sites or Companies

5. RESTRICTED information is not to be transmitted via the Internet. RESTRICTED information will be stored in locked wooden or steel furniture. It can be sent by Royal Mail or other appropriate carrier but should be sent to a named individual under single sealed cover with no protective marking on the outside. RESTRICTED documents must not be sent over the internet but they can be sent by fax within the UK if the intended recipient is on hand to receive it. Disposal should be by shredding.

6. RESTRICTED information may normally be faxed within Great Britain. However a few simple precautions are advisable, for example:

- a. Ensure that the addressee or an authorised representative of the department is available to receive the fax before it is transmitted.
- b. Do not send a RESTRICTED fax too late in the day or to unoccupied premises.
- c. Ensure that the dialing code and number are keyed accurately to avoid sensitive information being misdirected

Transmission Abroad

7. Information which merits a RESTRICTED marking should be sent by post in a single envelope. The RESTRICTED marking must not appear on the outside of the envelope which should be addressed to the appropriate person by name.

Custody

8. When not in use, RESTRICTED information should be placed within a locked container, cupboard or store and the keys appropriately secured.

Use of Information Technology (IT)

9. RESTRICTED information and data should not be processed on networked machines which have not been formally accredited by OCNS. RESTRICTED information may be processed on laptops or stand alone desktop machines provided these remain isolated and are not subsequently connected, temporarily, to a network, for example, to link to a networked printer. The security and storage of laptops and removable media such as disks and USB drives should be in keeping with the protective security standards set out in this annex.

10. Users must ensure that IT equipment is adequately protected when it is removed from a site or company premises. This is particularly relevant in the case of attractive assets such as laptops which are vulnerable to theft from vehicles, hotel rooms or private residences.

11. Similar levels of care must be exercised when devices, eg laptops and PDA's which have been used to process RESTRICTED information are no longer required. Hard drives should be cleaned to a satisfactory standard using a Government approved package and storage media should effectively destroy by shredding or disintegration.

12. Further advice on the management and security of IT facilities being used for RESTRICTED data can be requested from OCNS at any time.

Application of the protective marking

13. Those originating RESTRICTED documents should ensure that the RESTRICTED marking appears prominently at the top and bottom of each page, including the front and back covers of a multi page document. Printed in uppercase, in 14pt bold, is the normal standard. In the case of removable media for use with IT, the protective marking should be annotated on the item in a way that remains evident to users and such items should be stored and protected accordingly.

Loss or compromise

14. Any loss of RESTRICTED assets must be reported without delay to OCNS. Similarly, if it is thought that RESTRICTED information may have been compromised the circumstances should be reported immediately to OCNS.

Destruction

15. As soon as no longer required, RESTRICTED information should be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces and mixing thoroughly with other waste. Unwanted RESTRICTED assets that cannot be effectively destroyed should be returned to the Contracting Company or OCNS.

Further Advice

16. Further advice on the protection and management of RESTRICTED information is available through a Company Security Manager or the relevant contact at OCNS.

GUIDANCE ON THE PROTECTION AND MANAGEMENT OF CONFIDENTIAL INFORMATION

Introduction

1. Access to CONFIDENTIAL information should be strictly controlled and only shown to those people with an appropriate UK vetting clearance and following a 'need to know' principle. It should be confined to those employees whose access to the information is essential for the purpose of their duties.

Personnel Security

2. Employees and contractors having access to CONFIDENTIAL information should be warned that the Anti-Terrorism, Crime and Security Act 2001 includes provisions prohibiting the disclosure of sensitive information relating to nuclear security. This reflects the importance of safeguarding information from damaging disclosure which could prejudice the security of nuclear sites and nuclear material on sites or being transported anywhere in the world. Such disclosures could assist terrorists or others intending to attack or sabotage nuclear sites or steal nuclear material.

3. Section 79 of the Act makes it an offence to *intentionally* or *recklessly* disclose information which might prejudice the security of a nuclear site and nuclear material, whether on site or being transported, including on board a British ship.

Transmission within Sites or Companies

4. CONFIDENTIAL information may NOT be transmitted within sites and companies are to ensure that no unauthorised person can have access to this information. CONFIDENTIAL data should not be placed on an IT system and NOT transmitted by an Intranet IT system.

Transmission Outside Sites or Companies

5. CONFIDENTIAL information is not to be transmitted via the Internet. CONFIDENTIAL information should be stored in approved containers. It can be sent by Royal Mail or other appropriate carriers but should be sent to a named individual under a double cover with no protective marking on the outside envelope. CONFIDENTIAL documents must not be sent over the internet. Disposal will be by shredding using an appropriate device.

6. CONFIDENTIAL information may not be faxed.

Transmission Abroad

Custody

8. When not attended, CONFIDENTIAL information should be placed within an approved container appropriately secured.

Use of Information Technology (IT)

CONFIDENTIAL information must not be introduced into any IT system without the prior authorisation of OCNS