

**NOT PROTECTIVELY MARKED**

**Office for Civil Nuclear Security**

# **Civil Nuclear Security Supplement No 5**

## **Guidance for contractors on the protection and management of Restricted information**

Issue No 1 – August 2007

**NOT PROTECTIVELY MARKED**

## Guidance for contractors 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 of contractors having access to RESTRICTED information should be warned that the Anti-terrorism, Crime and Security Act 2001 includes provisions that prohibits the disclosure of sensitive information relating to nuclear security. This reflects the importance of safeguarding information from 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 with malicious intent to attack or sabotage nuclear facilities 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 of RESTRICTED information within sites or companies

4. RESTRICTED information should be transmitted within sites and companies in a manner that ensures that no unauthorised person can gain access to it. RESTRICTED data should not be placed on any IT system or transmitted over any Intranet system unless the system has been formally accredited by OCNS to store and process protectively marked material. Under no circumstances should RESTRICTED information be relayed over the Internet.

### Transmission of RESTRICTED information outside sites or companies

5. With the exception of the mandatory notifications of the transport of Category III nuclear material, for which a specific dispensation from OCNS applies in appropriate cases\*, RESTRICTED information may not be transmitted via the Internet. RESTRICTED information may be sent by ordinary post in a single envelope. The word RESTRICTED must not appear on the outside of the envelope.

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

- a) ensure before it is transmitted that the addressee or an authorised member of the receiving organisation or department is available to receive the fax;
- b) do not send a RESTRICTED fax too late in the day, when the addressee or their representative may not be available or to an unoccupied office or premises;

- c) ensure that the dialling code and number are keyed accurately to avoid sensitive information being misdirected.

**Transmission abroad**

7. With the exception of mandatory notification of the transport of Category III nuclear materials, for which the Internet or facsimile is approved, information which merits a RESTRICTED marking should not be normally sent abroad. Where permitted, it 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 access to the keys must be strictly controlled.

**Application of the protective marking**

9. 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. Printing the marking in uppercase, 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**

10. Any loss or of RESTRICTED assets must be reported without delay to OCNS, and to the Contracting Authority. Similarly, if it is thought that RESTRICTED information may have been compromised in any way, the circumstances should be similarly reported. Contracting authorities and contracting companies subject to the Nuclear Industries Security Regulations 2003 are to report breaches of security to OCNS within 24 hours.

**Destruction**

11. When it is 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 are to be returned to the Contracting Authority or OCNS for appropriate disposal.

**Use of computers**

12. The use of computers to process protectively marked information, for the purposes of a classified contract, is covered by CNSS No 3.

**Further Advice**

12. Further advice on the protection and management of RESTRICTED information is available through the Security department of the Contracting Authority or the relevant contact at OCNS.

(\*see document “Technical Requirements: Minimum Standards for the Physical Protection of Civil Licensed Nuclear Sites, other Nuclear Premises and Nuclear Material in Transit”, Part Four, paragraph 4.1.20. This dispensation covers a very specific area and not all users of this CNSS will hold a copy of the referenced document)