

NOT PROTECTIVELY MARKED

Office for Civil Nuclear Security

Civil Nuclear Security Supplement No 3

The use of computer systems in classified contracts in the civil nuclear industry

Issue No 1 – August 2007

NOT PROTECTIVELY MARKED

The use of computer systems in classified contracts in the civil nuclear industry

Introduction

1. There is a requirement, within the Civil Nuclear Industry, that a firm awarded a classified contract may only process protectively marked information on standalone computers under approved arrangements. The restriction placed on the use of contractors' IT systems stems from a national policy that computer systems storing, processing and, sometimes, forwarding protectively marked information, must be formally accredited to Government standards. In the civil nuclear industry such accreditation work is performed by OCNS.
2. In the circumstances presented by some of the larger contracts now prevailing in the industry, this restriction is proving burdensome. Consequently, it has become necessary to review the policy on the use of computers and, if possible, to allow for wider use of computer systems on classified contracts. This will continue to necessitate the formal accreditation of some contractors' systems. The accreditation process ensures that a computer system used for protectively marked information incorporates appropriate safeguards, standards and equipment to ensure the security of the information involved. Obviously, the higher the protective marking the more stringent the accreditation requirements that are necessary.
3. While a stand-alone computer can be covered by a fairly simple, almost generic, accreditation document, accreditation of a network of computers is more complex, can be time consuming and is, therefore, a more costly process.
4. Given such circumstances, where computer technology has become an essential feature of contract management and delivery, it is acknowledged that some relaxation of the restrictions on the use of computers in classified contracts could be beneficial. Accordingly, it has been decided to permit wider use of computer equipment by firms engaged in classified contracts and the rules for this approach are set out below.

General provisions and limitations

5. From 1 January 2006 firms granted a classified contract will no longer be limited to the use of stand-alone computers to store and process protectively marked information pertinent to the contract. However, as noted in the following paragraphs, there must be some limitation on the use of computer systems.
6. Most companies eligible for a classified contract will usually have in place a corporate data network. These are usually quite large and often with diverse connections to other systems including the Internet. It is neither feasible nor desirable for OCNS to accredit such networks. Moreover, as such networks would have to be accredited before any protectively marked material could be installed, and accreditation of significant networks takes time, there could be significant cost and an adverse impact on the start of a contract. For this reason protectively marked information *is NOT to be held or processed on existing company or corporate networks, without prior OCNS approval*

7. This limitation does not, however, preclude a contracting firm from creating a small discrete local area network (LAN) specifically for use on the classified contract. Such a network should, however, have no connection to any other computer system, network nor to the Internet. A network that conforms to these parameters would be relatively easy to accredit and the time taken for accreditation should not impact too much on the start of the contract.

Accreditation for RESTRICTED contracts

8. The process of accreditation is resource intensive and OCNS does not have sufficient specialist staff to perform the work for every classified contract for which a small, discrete network might be required.

9. As outlined in CNSS No 2, it is now possible, in the case of RESTRICTED contracts, for the Contracting Authority to perform the checks and inspections necessary for assurance that the Contracting Company is suitable to hold the protectively marked information and this concession is being extended to cover the accreditation of computer systems security at a similar level.

10. If, from January 2006, a contracting company is prepared to configure a discrete system or network to facilitate its work on the contract at RESTRICTED level, OCNS will usually allow the Contracting Authority to conduct an accreditation of that dedicated computer system or network, subject to the limitations outlined in the following paragraphs.

11. This extension of authority for companies in the civil nuclear industry is limited to contracts that involve information or material that attracts a protective marking *no higher than* RESTRICTED.

12. The accreditation work is to be performed by a member of the Contracting Authority's security staff who has successfully attended a formal Accreditor's Course under OCNS sponsorship.

13. A copy of the Accreditation Document Set (ADS), for each accredited system is to be retained and be available for inspection by OCNS.

14. A record of the company granted accreditation is to be retained and a copy of the signed Accreditation Certificate is to be sent to OCNS, together with the copy of the contract and the Security Aspects Letter relevant to the contract.

15. The accreditation is to be reviewed at six-monthly intervals to ensure that the circumstances remain consistent with terms on which the accreditation was originally based.

Register of companies and accredited systems

16. OCNS will keep a register of those companies that have had a computer system, (processing RESTRICTED information), accredited under this scheme. In appropriate circumstances the information on the register will be available to the other companies in the industry. It is imperative therefore that details of classified contracts and of systems that have been "accredited" under this scheme are passed to

OCNS in a timely manner.

17. This registration system will work in a manner similar to that adopted by the Security Service for companies on the X List. Should the List X scheme cease to operate in the future, the OCNS register of companies will provide a valuable record for the civil nuclear industry. It is anticipated that MOD will apply a similar arrangement for its contractors. OCNS will, therefore, maintain liaison with MOD on this aspect.

Accreditation and clearance activities

18. To minimise any delay to the start of a contract due to the need to carry out an accreditation, companies intending to let a RESTRICTED contract should gather as much information as possible from the short-listed companies. A questionnaire devised by British Nuclear Group to assist in this data capture is attached at Annex A to this supplement for information. British Nuclear Group has agreed that other companies in the civil nuclear industry may use or adapt the questionnaire to suit their own needs. OCNS proposes that the format could be usefully applied in gathering company information from prospective operators of a RESTRICTED LAN.

19. The Contracting Authority can assist the chosen contractor with the production of the necessary ADS. If the information is gathered in advance the time taken to produce the ADS will be minimised.

Contracts CONFIDENTIAL and higher

20. The extension of authority outlined above *does not* apply to contracts that involve information attracting a protective marking of CONFIDENTIAL or higher. As is usual with contracts of this nature OCNS will, in addition to the usual security checks, also carry out any necessary accreditation and act as the Security Adviser for the contract.

21. However, the cost of providing a discrete computer network that could be accredited for higher levels of information could be significant and the time necessary to perform an accreditation at this level could impact severely on the start of the contract. Depending on the circumstances, firms awarded contracts involving such information may well be advised by OCNS to continue the use of stand-alone equipment and removable storage media.

Firms contracted to more than one operator

22. While a firm is contracted to just one company in the civil nuclear industry, irrespective of the number of contracts between them, that Contracting Authority acts as both the Security Adviser and the Accreditor for the firm under contract. If, however, the firm under contract with one nuclear operator takes on a contract for another nuclear operator there is scope for confusion on the part of the contractor and the possibility of conflicting advice being given by the two contracting authorities. To avoid such conflict OCNS should be informed when such a situation occurs. OCNS will then assume the responsibilities of Security Adviser and Accreditor for the contractor.

Close of contract

23. At the end of the contract the contracting authority's accreditor is to ensure that the contractor's computer system is completely wiped in accordance with HMG standards of protectively marked information. In this respect OCNS advice is to be sought as necessary and OCNS is to be informed when the closure is satisfactorily completed.

Please complete all questions below by marking entering a cross in the appropriate box.

1. Information Classification	Yes	No
a. What level of information will be processed by your Company at the location specified?		
Commercial	<input type="checkbox"/>	<input type="checkbox"/>
Restricted	<input type="checkbox"/>	<input type="checkbox"/>
Confidential	<input type="checkbox"/>	<input type="checkbox"/>
Secret and above	<input type="checkbox"/>	<input type="checkbox"/>
b. How many people will potentially have access to above information? (enter number)		
c. How many people will be working on the above information? (enter number)		
d. Is the location/site where the information will be processed LIST X approved ¹ ? (If the answer is YES, then proceed to the Physical Security Questionnaire)	<input type="checkbox"/>	<input type="checkbox"/>
 2. Standards	Yes	No
a. Is your Company ISO17799 accredited?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes then please go to question 15		
 3. IT Security Policy	Yes	No
a. Does your Company have an IT Security Policy?	<input type="checkbox"/>	<input type="checkbox"/>
b. Is the Policy endorsed by Board/Executive/Directors?	<input type="checkbox"/>	<input type="checkbox"/>
 4. Organisation of Information Security	Yes	No
a. Does your Company have a nominated/appointed Security Officer/Controller ² ?	<input type="checkbox"/>	<input type="checkbox"/>
b. Does your Company have a nominated/appointed IT Manager?	<input type="checkbox"/>	<input type="checkbox"/>
c. Are internal/external audits/assessments carried out on your Information Security System?	<input type="checkbox"/>	<input type="checkbox"/>
 5. Human Resources Security	Yes	No
a. Are employees working with PMI cleared to the appropriate level ³ ?	<input type="checkbox"/>	<input type="checkbox"/>
b. Does your Company provide security awareness, education and training to employees and contractors?	<input type="checkbox"/>	<input type="checkbox"/>
 6. Communications and Operations Management	Yes	No
a. Is your IT support and/or maintenance provided by a third party?	<input type="checkbox"/>	<input type="checkbox"/>
b. Does your Company have and implement an Anti-Virus policy?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes please give details of the Anti-Virus software used		

¹ LISTX – location or facility formally audited and approved by the Government Security Services/Regulator to process PMI above RESTRICTED.

² A Security Controller is the official Government designation for the person within an organisation who discharges security responsibilities against the Manual of Protective Security at a List X facility in order to protect Protectively Marked Information² or sensitive technologies or materials.

³ Access to Commercial information and protectively marked information up to Confidential requires Basic Identity and Integrity Check, access to Secret requires SC clearance and access to Top Secret requires DV clearance.

NOT PROTECTIVELY MARKED

Civil Nuclear Security Supplement No 3

	Yes	No
c. Does your Company have and implement a Back-up policy?	<input type="checkbox"/>	<input type="checkbox"/>
i. Is marked media which may be re-used overwritten with authorised software?	<input type="checkbox"/>	<input type="checkbox"/>
d. Does your Company have and implement a formal information exchange policy with both internal and external entities (i.e. exchange of information via email)?	<input type="checkbox"/>	<input type="checkbox"/>
7. Access Control	Yes	No
a. Does your Company implement Access Control management (i.e. user access rights, access to applications etc)?	<input type="checkbox"/>	<input type="checkbox"/>
b. Does your Company implement Password management?	<input type="checkbox"/>	<input type="checkbox"/>
c. Is your Company network connected to the internet?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes, please give details of your firewall installed		
	Yes	No
d. Is your Company network distributed across the UK?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes, please provide a network diagram		
	Yes	No
e. Will the network or PC processing the information be connected to any other 3 rd party network including BNFL?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes, please provide the name of the Company and type of network connection		
	Yes	No
f. Is the information relevant to this contract processed on your Company network?	<input type="checkbox"/>	<input type="checkbox"/>
g. Is the information relevant to this contract processed on a standalone computer (i.e. not connected to a network)?	<input type="checkbox"/>	<input type="checkbox"/>
h. Is your network Government Accredited to process Protectively Marked information?	<input type="checkbox"/>	<input type="checkbox"/>
i. Will any wireless facility be used for the processing of PMI in this contract?	<input type="checkbox"/>	<input type="checkbox"/>
8. Encryption	Yes	No
a. Will the information processed for the contract be encrypted?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes please give details of encryption software used		
	Yes	No
b. Will removable media, used to store and/or transmit information for the contract, be encrypted?	<input type="checkbox"/>	<input type="checkbox"/>
If Yes please give details of encryption software used		
9. Change Control	Yes	No
a. Does your Company have and implement formal change control procedures (i.e. changes to existing systems, introduction of new systems, new software)?	<input type="checkbox"/>	<input type="checkbox"/>
10. Security Incident Management	Yes	No
a. Does your Company perform auditing and monitoring (event logging) across your network?	<input type="checkbox"/>	<input type="checkbox"/>
b. Are information security events/incidents monitored and reported?	<input type="checkbox"/>	<input type="checkbox"/>

NOT PROTECTIVELY MARKED

Civil Nuclear Security Supplement No 3

- | | | |
|--|--------------------------|--------------------------|
| 11. Disaster Recovery | Yes | No |
| a. Does your Company implement Disaster Recovery? | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Are back-ups stored at a different location from the location processed? | <input type="checkbox"/> | <input type="checkbox"/> |
| 12. Compliance | Yes | No |
| a. Does your Company's Information Security Management System (ISMS) comply with all statutory, regulatory and contractual obligations (i.e. Data Protection Act, Computer Misuse Act etc.)? | <input type="checkbox"/> | <input type="checkbox"/> |
| 13. Media Management | Yes | No |
| a. Does your Company implement media management (i.e. removal, transfer, disposal, storage, document marking and labelling of media)? | <input type="checkbox"/> | <input type="checkbox"/> |
| b. How is all your PMI media used in this contract destroyed? | | |
| 14. Mobile Computing | Yes | No |
| a. Will laptops be used for the storage of PMI for this contract? | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Will the appropriate security arrangements for storage/protection of the above laptop be implemented? | <input type="checkbox"/> | <input type="checkbox"/> |
| 15. Additional Information | Yes | No |
| a. If this contract requires the processing of PMI does your Company's ISMS comply with the Nuclear Industries Security Regulations 2003 (Part 4 Regulation 22)? | <input type="checkbox"/> | <input type="checkbox"/> |
- If you wish to supply any additional information please state here: