DCI GEN 78/97 Procedures for Internet Connection (U)

[D/D PoI(ICS)/40/13/5/1: [redacted]]

Introduction

1. There is evidence of continuing interest in MOD in making use of the Internet. A number of business areas are beginning to establish connections. There are significant benefits in connecting to the Internet, but also potential risks. A Departmental policy on the use of the Internet is being developed by DGMO and it is hoped that this can be approved and promulgated by the summer. It is also planned that the DGICS Catalogue will offer a selection of full Internet services as a communications service at the same time.

2. Users contemplating connection are advised to await the policy and the Catalogue service, but those who believe that they have a pressing need to proceed with connection in the interim must follow the procedures and observe the restrictions described in the following sections.

Planning the Connection to the Internet

3. The following procedures should be followed:

a. Prepare a brief business case for the appropriate budget manager, showing how any additional costs can be justified. Obtain financial approval.

b. Draft system security policy and security operation procedures and seek the approval of the appropriate security authority to proceed. Refer to JSP440, Chapter 5 and DCI **4/96**.

c. Seek the advice of the sector Coordinating Installation Design Authority (CIDA - see below) on the installation criteria.

d. Carry out the procurement procedure for the service through single sector procedures; where a number of Internet accesses are required procedures for using the existing enabling contractors for IT services can be used, indicating any preference for one of the Service Providers.

e. The Service Provider will liaise direct to implement connection and allocate domain name.

f. Implement procedures for the management and monitoring the use of the Internet.

Security

4. The Internet is open to a world wide computing fraternity and until such times that accredited security products are available for government use, it is necessary to restrict its use to unclassified MOD business. In general, to prevent unauthorised access to MOD data, Internet connections and applications must be run on machines which are dedicated to the Internet role and which hold no protectively marked or caveated material. The security requirements for all connections to the Internet are contained in Chapter 5 of JSP 440 (The Defence Manual of Security Volume 3 Information Technology Systems.) Further details on Computer Security can be found in DCI **4/96**.

5. The approved method of connection to the Internet is by the use of a machine dedicated to processing Internet data. The security requirements of JSP440 are summarised as follows:

a. A System Security Policy (SSP) and Security Operating Procedures for the Internet machine must be produced. Proforma for these documents are contained in JSP 440.

b. The approval of the appropriate Security Authority must be obtained before equipment is connected to the Internet.

c. The machine must be clearly marked as being for UNCLASSIFIED use only.

d. Care must be taken to ensure that information held or created on the web site by virtue of its nature or aggregation, does not warrant upgrade to a higher level of protective marking.

e. The transfer of data from the machine dedicated to the Internet to other MOD IT systems must be achieved by manual methods using either hard copy or floppy disks, i.e. an air gap must exist between the two machines. It is important that all such material must be checked for the presence of viruses and other malicious software prior to loading onto the MOD system. It is recommended that anti-virus software is installed on the Internet machine so that the integrity of imported software can be checked immediately. In addition good 'hygiene' practices should be carried out by routine checks for viruses.

Coordinating Installation Design Authorities

6. Coordinating Installation Design Authorities (CIDA) exist to ensure that Information Technology and Office Automation systems are installed to a common standard. CIDAs are responsible for installation approval of all new Internet connections and their early advice should be sought. Points of contact in CIDAs are:

a. *MOD HQs and MOD(PE):* ICS(Infra)Comms 1 Tel: [redacted]

b. *Royal Navy:* Directorate of Naval Shore Telecommunications Tel: [redacted]

c. *Army:* Communications Projects Division, CIS Eng Group Tel: [redacted]

d. *RAF:* RAF Signals Engineering Establishment Tel: [redacted]

7. If defence telephone networks are to provide the connectivity, prospective users must consider the ability of these networks to accommodate the increased loading of existing lines and of the budget holder's ability to pay for any additional lines and infrastructure that may be required. The appropriate CIDA can advise on line loading and operating costs.

8. When considering the cost of providing an Internet facility, allowance needs to be made for the following:

a. Normally a dedicated, stand alone, personal computer is required. Whilst it is possible to access the Internet using any machine, a high performance multi media machine may be more effective for some applications.

b. A modem or appropriate network card is required. Generally the cost of a modem increases with its performance, however high speed modems can reduce call duration and consequent running costs.

c. A printer may be needed.

d. Installation costs arising from the provision of furniture, laying of cables etc.

e. Call charges.

f. Connection and rental charges.

Service Providers

9. Access to the Internet is obtained through an agency or contractor known as an Internet Service Provider. In order to simplify the procurement of Internet services and obtain best value for money and quality of service it has been decided that the number of Service Providers to the MOD for new Internet connections will be RESTRICTED, through competition, to a small number. On completion of the competitive tendering process, the list of approved Service Providers will be published in the DGICS catalogue with comprehensive details of services offered and costs. Full details will also be published in JSP343, the MOD ICS Handbook.

10. In the interim sectors should take advice on the suitability of Service Providers from their single sector focus for the Internet.

Creating Internet Pages

11. The process of producing a Home Page suitable for publication on the WWW involves the use of word processors or text editors which produces documents written in a form know as Hypertext Markup Language (HTML). In anticipation of future policy and to allow the MOD Library a degree of coordination, users producing home pages should inform the MOD Library of their current and future published material. Guidance on the production of WWW pages is to be obtained from the staff of the MOD Chief Librarian, tel: [redacted].

12. Before material is published on the Internet users must seek advice and editorial clearance from their respective DPRs for the single Services and D Info D for the Centre Staff and PE.

Improper Use of the Internet

13. Internet facilities provided by the MOD are for the pursuit of official business. Care must be taken that no messages are made publicly available that may be considered to be defamatory in any way and expose the sender or the MOD to retribution, in addition the use for personal advantage of Internet facilities provided by the MOD is not permitted, and may result in disciplinary action being taken against the user. Technology is available through most Internet Service Providers to monitor access, provide statistics and bar access to non work-related WWW sites. Types of prohibited activity is at the ANNEX to this DCI.

14. Queries relating to this instruction should be passed to: ICS(Pol)Sec1b, DGICS, [redacted] or BT [redacted].

ANNEX

Prohibited Use of Internet Services

1. The use of Internet services in the following types of activities is specifically prohibited.

a. Illegal, fraudulent, or malicious activities.

b. Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with MOD.

c. Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitations of business or services, sales of personal property.

d. Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.

e. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.

f. Storing, processing, or distributing classified, proprietary, or other sensitive or for official use only information on a computer or network not explicitly approved for such processing, storage, or distribution.

g. Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.

h. Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.

i. Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.

j. Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.

k. Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

2. These activities may result in disciplinary action being taken against the person found misusing the Internet service for such purposes.