4/96 Computer Security — MOD Security Policy for Connection to the Internet or Other Public Data Networks (U)

[D/DPol(ICS)/47/8/2: [redacted]

Introduction

1. Connection to public data networks such as the Internet is becoming a requirement for many MOD and Service applications. Whilst the need for this is fully accepted, it should be recognized that such connections are inherently insecure. Some special security measures such as firewalls can give some degree of protection against unauthorized access, but at present, there is currently no fully trusted method of protecting systems which are so connected. Users of any MOD or Service system considering connection to the Internet or other public data networks must understand the risks of taking such action and ensure that the security policy detailed below is followed in all cases. This DCI upgrades the procedures detailed in Chapter 5 of JSP 440 — The Defence Manual of Security Volume 3 — Information Technology Systems. General Defence policy for the provision and use of Internet connections will be promulgated shortly by DGICS as a MOD ICS policy statement in their IP series of documents. This document should also be consulted whenever a requirement to connect to Internet arises. It will be incorporated in JSP 343.

Aim

2. The aim of this DCI is to detail the present MOD security policy for connection to the Internet and other public data networks. In effect it cites the security conditions under which connections to such networks may be permitted.

Authority to connect

3. Authority to connect to the Internet or any public data networks from within MOD and the Services is retained at Sector level. Applications are to be made through the local IT Security Officer (ITSO), Branch Security Officer (BSO) or equivalent to the appropriate sector security authority as follows:

Army	G2 Sy2 (Information) HQ Land
Navy	DNSyICP.X6 2SL/CNH
RAF	DDSyCIS(RAF) HQLC
HQ, PE & Agencies	HQ Sy 3a

It should be noted that the agreement of the relevant sector communications security authority and in many cases, the Coordinating Installation Design Authority (CIDA) will also be required. Where individual or interconnected systems cross sector boundaries, the agreement of all participating sectors is required.

Connection summary

4. MOD systems accessing the Internet should be dedicated to the purpose, typically a stand-alone PC and process only non-protectively marked information. The connection of the accessing system to any other MOD systems is in most cases, not permitted. If, however, it is desired to connect any existing MOD system directly to the Internet, this may be possible by use of firewalls. MOD systems processing information protectively marked at RESTRICTED must obtain the prior approval of the appropriate sector security authority and only use a firewall product (see para 6) which has been accredited by that authority. Under these circumstances, the Internet or other public data networks are not to be used to carry protectively marked information. Connection to systems processing information protectively marked at CONFIDENTIAL and above is strictly prohibited. Communications bearers must be approved by the appropriate security or Comsec authority.

MOD Policy for connection

5. Direct or indirect connection to the Internet and other public data networks may be permitted under the following conditions:

a. The system to be connected should normally be dedicated to the role and process only non-protectively marked (i.e. unclassified) information. This also applies to information stored on or transmitted by MOD World Wide Web (WWW) or other news and bulletin board servers. If any official information processed is not for public view, then use of firewalls must be considered.

b. If it is desired to connect an existing MOD system directly to the Internet, this system should be unclassified and information not for public view should be segregated by use of a firewall or similar product, the sophistication of which will depend on the quantity and type of information held on the system. Other means of protecting the 'non-Internet' data, should also be considered.

c. The establishment of a dedicated Internet system at RESTRICTED level or higher is not permitted. Users of stand-alone unclassified systems attached to the Internet should therefore ensure that the information held or created, does not, by virtue of its nature or aggregation, warrant upgrade to a higher level of protective marking. If this does occur, the information should be removed to a different system.

d. If, exceptionally, it is desired to connect an existing MOD system which processes RESTRICTED information to the Internet, the firewall used to segregate and protect this information must be accredited. The approval of both the sector IT security authority and the Comsec authority must be obtained prior to connection. In addition to clearly detailing the requirement and the protectively marked information involved, the case to connect must demonstrate fully that an evaluation of the risks has been undertaken and any residual risk accepted. If after consideration, an 'approval to operate' can be granted, this will be provided in writing by the appropriate sector security or Comsec authority.

e. The direct or indirect connection of any IT system processing/holding information (either on the basis of individual items or by aggregation) protectively marked at CONFIDENTIAL and above is prohibited.

f. The processing of any official information other than that for which the system is authorized, is prohibited.

g. All systems planning to connect to MOD controlled services, including those handling only unclassified information, must have a System Security Policy (SSP), supported by appropriate Security Operating Procedures (SyOPs), which are to be approved by the appropriate sector security authority. Systems connecting to non-MOD controlled services will need to assure the appropriate sector security authority that no information which is not for public view will be released.

h. The provision of telephone or other communications lines which may be used to provide Internet access will vary depending on local circumstances. Use of the Government Telecommunications Network (GTN) to connect stand alone systems to CCTA's GTNet or the use of direct exchange lines (DELs) to commercial hosts are alternatives. In all cases, however, potential users must seek the advice of the appropriate sector security or Comsec authority in the first instance. The authority will if necessary consult with the local CIDA to determine equipment and bearer installation standards.

i. Passage of information from the Internet accessing system to other unconnected MOD IT systems must be achieved by hard copy or floppy disk. In the latter case, all disks must be checked for the presence of viruses and other malicious software prior to uploading. Extreme care must be taken if importing executable code.

j. Electronic mail (E-Mail) addresses should wherever possible conform to the naming and addressing standard as specified by the Defence Message Handling Sub Committee (DMHSC), should be disclosed with discretion and only used for official business.

k. Any abnormal security related conditions identified by a user must be reported to the security authorities as well as to technical support staff. The normal incident reporting methods are to be applied.

Use of Firewalls

6. As stated above, the connection of existing RESTRICTED systems to the Internet will require the protection offered by an accredited firewall. Research into this area is currently being carried out by DRA Malvern and CESG. Therefore, if approval in principle to connect a RESTRICTED system has been given, sector security authorities should discuss their special requirements with these organizations.

Enquiries

7. Any comments or queries concerning the contents of this DCI should be made in the first instance to the local IT security contact.