

A controlled environment

Many organisations could unknowingly be contravening the rules of the new Export Control Act. *Alex McLoughlin* reports.

All the signs are that tens of thousands of export control offences will already have been committed by British exporters, finance houses, academics, technologists and others who are ignorant of — or have underestimated the scope of — the new Export Control Act.

The new Act came into force on 1 May this year, but the government's message has not got through to the directors of many hi-tech companies, software houses and defence organisations that the future of their business could be on the line if their output reaches the wrong hands.

Intolerable odium

Because of current perceived terrorist threats, any organisations thought to have breached export controls will face intolerable odium from parliament, press and public.

Defence industry directors who have not personally satisfied themselves that the Export Control Act has been thoroughly understood and acted upon by their organisation, may well find that they have no legal defence in court if some dealer somewhere ships their products to an embargoed destination. Their own board is likely to be even more unforgiving if defence contracts are lost in Britain, the USA and elsewhere.

When will the honeymoon end?

Softly, softly seems to have been the government's approach to the most far-reaching changes in export control legislation since 1939, but how long will this honeymoon last?

Many hi-tech and defence exporters will be caught unawares if a due diligence exercise or an internal or external audit uncovers inadequacies in their compliance programmes.

When an appropriate case provokes enforcement action by HM Customs it may well be too late to do anything other than make a voluntary disclosure to the authorities.

Dealing with the issue of "Who armed Saddam Hussein?"

To put the Act into context, one has to cast one's mind back to the Iraqi "super gun" affair and Sir Richard Scott's report on the export of defence and dual-use equipment to Iraq in February 1996. The Parliamentary debate on this report almost brought about the collapse of John Major's government.

The issue was: "Who armed Saddam Hussein?". The new Export Control Act is the direct result of this issue and it also updates the old 1939 Act by subjecting the statutory instruments that will be issued to parliamentary scrutiny to create "transparency". Some of the tenets of the Official Secrets Act also seem to have been embodied in the new Export Control Act.

The new Act imposes controls on "Technical Assistance Overseas" which is defined as "services used or capable of use or provided, in connection with developing or using controlled goods or technology".

The Act also controls exports from the UK and the transfer from the UK of certain technologies (and by UK persons anywhere by any means other than by export).

Trafficking or brokering

The acquisition or disposal of goods that are themselves subject to export control, or activities that facilitate such acquisitions or disposals, are often referred to as trafficking and brokering. Any persons engaged in brokering will need a licence before they can act as facilitators or middlemen in arranging for arms or military related goods to be supplied between other countries.

Export controls now extend to technical data, documents, research and all forms of communication including those over the Internet and dictated oral disclosures, if they are in any way related to controlled technology or prohibited end uses.

Essentially this Act will control the export of goods and technology from the UK and extra-territorially if they are under the control of a "UK person". This puts a UK company, university or other organisation at as much risk in UK law as a US corporation and its subsidiaries abroad under the US Export Administration Regulations and anyone anywhere in the world using technology controlled under the US ITAR (International Traffic in Arms Regulations). The national and geographic bases of the two sets of regulations are however different.

New powers over technology and information transfer

The Act also gives the Secretary of State powers to require information, in addition to existing requirements. It also provides for the minister to introduce controls agreed in the EU or the United Nations relatively simply including an EU Joint Action agreed

in June 2000 on the transfer by any means of technology or information where the provider knows or is informed by government that the technology or information is intended for use in a weapon of mass destruction (WMD) or related missile programme.

The trade controls should be viewed as a response to dealers, brokers and traffickers who moved arms from the trouble spots of Europe to the trouble spots of Africa.

The extension of the transfer controls on technology, however, is a clear reflection of the dangers in today's world of proliferation, particularly by terrorists and rogue nations.

Almost anything except foodstuffs and medicines may be controlled by reasons of military use or use in manufacture, research or deployment of WMD. The onus will be firmly on the exporter not the Department of Trade and Industry (DTI). The Act provides for maximum penalties of up to 10 years' imprisonment in the event of a serious breach. Prosecutions will be made much easier.

The need for compliance programmes

Now companies must develop new compliance programmes and not rely on 10-year old procedures. This time they must also: exercise tight control over intangibles; train and vet key technical personnel; and closely assess any dealers in third countries with whom they share technology.

Not to have taken new compliance measures is at best legally "reckless" and may leave members of the company board of any public or private sector institution open to prosecution, with minimal legal grounds of defence if technology gets into the wrong hands.

Deadline of 1 May 2004

The new Export Control Act had a deadline of 1 May for companies and other organisations such as universities and research establishments (even within the NHS for example) to register or apply for new licences.

In many cases systems updates, training and internal controls had to be ready in a matter of weeks. For example, access to UK websites of technical information that is deemed controlled military technology or "controlled" in certain circumstances must be denied to all parties if certain security restrictions are not put in place.



Who will the Act affect?

Under the Act even carriers, banks, insurance companies and finance houses or consultants could be charged with criminality if embargoed destinations, restricted technology or WMD, missiles, etc are involved even if all transactions took place outside the UK.

Intangibles like software, drawings, faxes, e-mails and even telephone conversations must be controlled and possibly licensed in such circumstances.

During the passage of this Act there were vexed issues in the House of Lords and the Commons as to how this law will affect academia and whether it could affect "sustainable development" to the Third World. The DTI has now issued guidelines for academics and researchers.

The defence industry was particularly concerned about "brokerage" where British nationals who are resident in the UK or abroad will, for the first time, be held accountable if they transfer goods or technology contrary to policy from one country to another without ever touching the UK.

Licensing of controlled technical data

Less dramatic but much more common will be cases where controlled technical data is released to individuals from countries where a licence is needed (including

students, employees and clients within the EU) or where equivalent websites are accessed from abroad.

Companies also have some hard thinking to do in determining which sales are for "military use"; they need to classify which products are "designed or modified for military use" and which are "restricted" as opposed to "controlled" or "paramilitary".

Destinations need to be categorised as "general licence" or "sensitive" or "embargoed". The controls also apply where work on controlled products is outsourced and technical instructions are given by a British organisation to move controlled kit from a EU country to a non-EU country. A broken military item for example remains controlled if it is repairable, even if it was originally sourced outside the EU.

Are UK companies in compliance?

How many companies have complied with these new standards and which companies are they? I would hazard a guess that only a minority, even of the UK subsidiaries of large multinational organisations, have got it right. Most will have assumed that compliance with US extra-territorial export controls and/or preparing for next year's audit by their Japanese parent will be enough.

No way. A synthesis between these three types of control must be achieved and few companies have invested in developing the necessary expertise.

The DTI's new code

The actions required of companies to protect themselves have been closely defined in the DTI's new code of compliance. When we worked with DTI in the development of the original compliance code just after the Iraqi super-gun affair, no one in Britain or the USA anticipated the current situation.

In the wake of HM Customs' investigations at that time, hundreds of lives were ruined although most prosecutions were subsequently dropped. Alan Clark's "nod, nod, wink, wink" most definitely will not be repeated, in today's world, but you would be surprised how many sales directors think otherwise.

[Alex McLoughlin and his colleagues in the Tara Trade consultancy have more than 60 years' experience of UK, US, Japanese, EU, UN and other export controls. More information can be found at \[www.customsadvisor.co.uk\]\(http://www.customsadvisor.co.uk\).](#)