Australia Group

Awareness-Raising Guide

A. Introduction

I. Australia Group objectives

The principal objective of participants in the Australia Group[1] is to ensure, through national licensing measures for the export of sensitive chemicals, biological agents and dual-use chemical and biological manufacturing facilities and equipment, that exports of these items do not contribute to the spread (proliferation) of chemical or biological weapons (CBW).

Viewed from the supply side, proliferation is the flow of technology, equipment, expertise and strategic goods from countries that possess these commodities to countries that do not. It is in the interest both of companies and research institutes as well as their governments to ensure that sensitive items are not inadvertently supplied for use in CBW programmes.

Awareness on the part of industry has a key role to play in achieving this objective. Export control can only be effective when all parties involved (manufacturers, exporters, engineers etc.) support such control. The fight against the proliferation of weapons of mass destruction (WMD) and CBW terrorism requires maximum cooperation. It is essential that all parties should be aware of the risks associated with sensitive goods and the danger of their misuse. To develop that awareness is the purpose of this guide.

II. The role of the awareness-raising guide

Since the chemical and biotechnology industries are targeted by proliferators as a source of materials for CBW programmes, awareness-raising is crucial to effective export control. The aim of this guide is to raise awareness among exporters as well as people who work with sensitive items of the risks associated with chemicals, biological agents, materials, bio-technology plants and components, software and expertise that are usually used for civilian purposes but could also be misused in CBW programmes or for terrorist activities. It is equally important to raise awareness of the danger that nationals from countries suspected of proliferation might obtain expertise that could be used in CBW programmes.

[1] The Australia Group Participants are (2003): Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, the European Commission, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Cyprus, Republic of Korea, Republic of Turkey, Romania, Slovak Republic, Spain, Sweden, Switzerland, United Kingdom, United States.

Particular vigilance is required in the case of countries suspected of being engaged in CBW programmes. Such countries may not only seek to procure sensitive items or components directly but also attempt to procure them via third countries.

No reputable company wishes to be involved in the misuse of any goods it produces and/or supplies. This is not just a matter of export control but also in its own self interest. Responsible corporate export control means that companies assess transactions on the basis of plausibility. Plausibility is assessed on the absence of any inconsistencies in the data provided. The stated use is plausible when the item in question is appropriate in terms of its objective characteristics, when corporate information on the recipient/end-user is consistent with the stated use and when this use is credible in view of all other circumstances (e.g. available expertise, technical and economic utility, order documents, end-use certificates).

The following parameters are intended to help companies assess whether there is any risk of becoming inadvertently involved in CBW programmes and in what cases they may seek further advice.

III. Awareness-raising strategies

This guide is only one of many ways of informing exporting companies about the risks associated with supplying goods that might be misused for CBW activities. The fact that the Australia Group has made the fight against terrorism one of its goals and introduced a catch-all provision in its licensing guidelines to address this threat has greatly enhanced the significance of corporate knowledge about the declared end-use and end-user of sensitive items.

The control lists drawn up by the Group are a key aspect of export control in the chemical and biotechnology field. Under national and supranational legislation to enforce this regime, the export of listed items is in principle subject to licensing. Details are laid down in the national legislation of participating countries.

In addition, the Australia Group’s guidelines provide for catch-all control of non-listed goods. Exporters are required to notify the relevant authority if they have any knowledge suggesting that non-listed items may in part or in their entirety be intended for use in CBW activities. Since such information is clearly crucial, exporters are encouraged to investigate the facts of

the matter before any export takes place and, if their suspicions are confirmed, notify the licensing authority accordingly.

The parameters detailed in Section B below for determining the plausibility of export transactions may also be useful in ascertaining what information is available to the companies involved or where further inquiries might be useful also in the interest of the exporter. What parameters are relevant in a particular case depends on the type of company, product or transaction involved. Experience has shown it is advisable for companies to appoint one person to be responsible for coordination and supervision at management level as well as an additional contact person with whom the licensing authority can clarify specific matters.

Since the relevant parameters will vary from case to case, companies should adapt their export control arrangements accordingly. The examples of suspicious circumstances or behaviour given below are not intended to be an exhaustive list nor do they indicate whether a specific export transaction is subject to licensing.

B. Detecting attempted procurement

I. Attempts involving chemicals, biological agents, plants and components

Anyone who passes on chemicals, biological agents, materials, plants and components may unintentionally be assisting in the planning or implementation of a CBW programme. Hence special vigilance is needed to detect attempts to acquire such items for suspect purposes, with particular attention being paid to any suspicious behaviour or business transactions relating to the supply of such items.

Suspicious customer behaviour generally inconsistent with normal business practice

a) Inquiries are received from unknown/first-time customers whose identity is not clear, who respond reluctantly to questions regarding their identity or connections, or whose credentials are unconvincing.

b) The supposed customer appears to be non-existent, unknown to industry liaison bodies or company registration authorities and not listed in any telephone or trade directories, Internet websites or other sources of unclassified information.

c) The customer is unable/reluctant to provide details of other commercial entities with whom they have previously dealt.

d) The customer appears to lack the capacity to process the quality/quantity of goods ordered or the nature of the customer's business is inconsistent with the order.

e) The customer is reluctant to provide sufficient explanation or clear answers:
   - to questions about the intended use of plants, chemicals or components or about relevant commercial or technical aspects of the transaction
   - to questions about a plant's location or the site where a plant is to be built or components or equipment to be installed
   - to commercial or technical questions which are routine in business negotiations or documents.

f) The customer demands unusual and excessive confidentiality concerning the final destinations or specifications of the products, materials or plant components to be supplied. Other grounds for suspicion may include:
   - demands for excessive security arrangements/measures in view of the stated use
   - the customer's obvious unfamiliarity with normal security requirements for the handling of such materials or plant components
   - denial of access for the contractor to plant areas outside those specified in the contract under circumstances which seem suspicious.

g) The customer splits up a contract for plant construction or conversion without providing any satisfactory information about the full scope of the order and/or the final destination of the plant, or the customer requests completion of a project that has been partially installed by a different company.

h) The country of destination is suspected of being engaged in WMD proliferation, including diversion activities, or is implausible given the nature of the goods to be supplied.

Suspicious orders

a) The description of the goods is vague or meaningless, or the goods appear to be manufactured to an unnecessarily high specification.

b) The order itself is unusual in some way, e.g. the quantity or performance of the ordered spare parts significantly exceeds or falls short - without any satisfactory explanation being given - of the quantity or performance normally required for the stated end-use.

c) The declared value of the goods is inconsistent with normal business practice.

d) A plant or part of the equipment in an existing or planned facility is to be modified in a manner that would significantly change its production potential and enable chemical or biological weapons or precursors to be produced on the site.

e) The site at which plant components are to be installed is unusual given the type of equipment involved, or the site at which the equipment is to be installed is unusual given the type of plant involved.

Suspicious circumstances regarding the business environment

a) The circumstances of a transaction involving a middleman or final consignee are unusual and deviate from normal business practice, e. g. the exporter is an individual and the quantity of goods to be supplied suggests they are to be used for manufacturing purposes.

b) The export documents do not match the information provided on the consignee or the description or quantity of goods to be supplied, or they are not of the company's usual standard. The export documents are not in the customary format or contain spelling errors or other simple mistakes.

c) Unusual shipping or labeling arrangements are requested by the customer, or the packaging or parts thereof are inconsistent with the type of transport envisaged or the stated final destination.

d) The packaging and handling arrangements do not match the stated use and/or final destination of the materials or components to be supplied, or similar suspicious arrangements.

e) Unusually favourable payment terms are offered such as a higher price, interest rates above normal market rates or lump-sum cash payment, or banking documents are not of the usual standard.

f) The amount of insurance paid on the shipment is not in line with normal business practice (either too high or too low).

II. Attempts involving know-how transfer from companies, research institutes and universities

Some countries misuse scientific cooperation in order to acquire expertise that is then used to develop and produce chemical weapons. Allowing scientists, students and technicians from countries engaged in proliferation access to universities and other scientific and technical institutions enables them to acquire a sound grasp of advanced technologies. The knowledge thus obtained may be used not only for civil programmes but for CBW activities as well.

Know-how transfer may occur through national and international conferences, trade fairs, special exhibitions, workshops, meetings, symposia, joint research and development projects as well as training and education programmes. Such events are also an opportunity to establish personal contacts that enable expertise to be obtained on an ongoing informal basis that does not arouse suspicion.

One type of know-how transfer are scientific and academic exchanges between industrialized countries and countries suspected of proliferation. Professional associations, technology centres and private and cultural initiatives also offer plentiful opportunities for contacts and information-sharing. Another way of obtaining expertise is to directly approach experts and/or technical personnel involved e. g. in the assembly or maintenance of production facilities. Know-how transfer is something that happens in every area of technology.

The following parameters may be useful in assessing whether the expertise being sought might be used for CBW activities. Special vigilance is recommended in the case of micro-organism cultivation and with regard to the handling, properties and storage conditions of pathogens or toxins. Particular caution is advised in all cases of unusual contacts and suspicious conduct.

In addition to those examples listed in Section I, suspicious behaviour generally deviating from normal practice includes:

a) the failure to make any request for the expert assistance or training usually required to install or operate plants or plant components;

b) requests for unusual and excessive confidentiality, e.g. reluctance to disclose information about the site of a (research) plant or the location where the contracted service is to be rendered;

c) in connection with sensitive chemicals or biological agents:
   - inquiries from nationals of countries suspected of proliferation about enrolling as students or seeking employment on research projects
   - requests from nationals of such countries to attend conferences and seminars
   - requests from unknown individuals, institutions and companies for help and advice in a specific area of technology and/or technical process;

d) requests relating to matters on which scientists, experts, research institute and laboratory staff etc. would not normally seek advice or information and for which unconvincing reasons or evasive explanations are given;

e) the failure
   - to explain or give convincing reasons why the technology/know-how transfer and training is being sought,
   - to explain or give convincing answers to questions regarding relevant commercial or technical aspects of a contract, or
   - to demonstrate that the requesting party possesses the expertise normally required for such projects;

f) arrangements which appear excessive in view of the nature of the services to be rendered or which demonstrate that the requesting party is clearly unfamiliar with the usual security requirements for such contracts.

III. Attempts linked to CBW terrorism

The Australia Group recognized the risk that chemicals, biological agents and production equipment might be misused for terrorist purposes long before 11 September 2001. The sarin attack on the Tokyo underground in 1995 and the ricin experiments detected in London in 2003 are only two examples of attempts by individuals or terrorist groups to cause injury and loss of life.

In a series of resolutions the United Nations Security Council has adopted specific measures aimed at combating terrorist activities by certain named persons and organizations. These resolutions impose a ban on providing technical consultancy, assistance or training to any listed natural and legal persons, groups or organizations in connection with military activities as well as on participating in the production or maintenance of any items for use as weapons and related purposes. These measures are targeted primarily but not exclusively at certain countries suspected of or known to be seeking to procure goods and technical know-how for WMD development and production and CBW terrorism. In supplying any goods or technical know-how to natural or legal persons listed in the relevant UN Security Council resolutions, companies should be aware of this background and apply appropriate corporate export control procedures.

In addition to the parameters listed in Sections I and II regarding export transactions and know-how transfer, companies should be aware of certain factors of specific relevance to preventing terrorism and take appropriate action.

They should be suspicious of requests and orders - especially those received from unknown parties - in which:

- the party's identity remains unclear because e.g. their letterheads are incomplete or have been copied into letters
- the only means of contacting the party is via a Post Office Box or mobile phone
- the party gives evasive answers to questions regarding their identity or can provide no convincing credentials
- the information provided about transport routes makes no geographical or economic sense
- the party is clearly not familiar with or ignores the security arrangements that are technically necessary for the handling or transport of chemicals or biological agents

- the party clearly lacks the know-how or facilities that are necessary or recommended for secure storage or use, especially in the field of highly sensitive technologies or technical processes.

Manufacturers and suppliers should seek to know, to the greatest extent possible, their customer before entering into contractual arrangements for the supply of materials and/or technology that could be used in the production of WMD or CBW terrorism.

C. Information / contact points

The Australia Group homepage: **www.australiagroup.net**
The Federal Office of Economics and Export Control homepage: www.bafa.de

In case of any doubt or questions concerning this guide, please contact the following official body responsible for export control in Germany:

Federal Office of Economics and Export Control
(Bundesamt für Wirtschaft und Ausfuhrkontrolle)
Frankfurter Str. 29-35, 65760 Eschborn
Phone: +49 6196 / 908-0; Fax: +49 6196 / 908-800
E-mail: poststelle@bafa.de
Internet: www.bafa.de