Nuclear Suppliers Group

Awareness Raising Document – July 2023

The aim of this document is to raise awareness, as broadly as possible - among exporters (and other suppliers such as original equipment manufacturers (OEMs)) and with access to sensitive items - of the risks associated with nuclear and nuclear-related goods, material, technology, software and expertise.

This document was endorsed by NSG Participating Governments at the 2023 NSG Plenary Meeting in Buenos Aires, Argentina.

A. Introduction

I. Nuclear Suppliers Group objectives

II. The role of the awareness-raising document

III. Awareness-raising strategies

B. Detecting attempted procurement

I. Attempts involving nuclear and nuclear-related goods, materials, facilities and technology

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

III. “Catch-All” controlling other items of proliferation concern

IV. Attempts linked to nuclear terrorism

C. Information / national authorities contact points

A. Introduction

I. Nuclear Suppliers Group objectives

The Nuclear Suppliers Group (NSG) is a group of nuclear exporting countries, which seeks to contribute to the non-proliferation of weapons of mass destruction by implementing two sets of guidelines for nuclear exports and nuclear-related exports. The NSG Guidelines aim to ensure that nuclear trade for peaceful purposes does not contribute to the proliferation of nuclear weapons or nuclear explosive devices, and that international trade and cooperation in the nuclear field is not hindered unjustly in the process.

Proliferation entails the flow of technology, equipment, expertise and strategic goods from countries that possess these commodities to countries that do not, and which are seeking to gain access to items for use in nuclear weapon programmes. It is in the interest both of industry, research institutes and their national governments, globally, to ensure that sensitive items are not inadvertently supplied for use in weapons programmes.

Industry and academia (i.e., universities, non-university research institutions, colleges, polytechnics, as well as individual or groups of scientists conducting research related to equipment, materials, software and technologies that may be subject to NSG export controls) have a key role in achieving this objective by raising awareness of the potential associated risks. Export controls can only be effective when all parties involved (manufacturers, exporters, management, researchers, engineers, etc.) are aware of and comply with such controls. The fight against the proliferation of weapons of mass destruction requires maximum cooperation. All parties must be aware of the risks associated with sensitive goods and the danger of their misuse. It is the purpose of this document to help develop a framework that encourages this awareness.

II. The role of the awareness-raising document

The aim of this document is to raise awareness, as broadly as possible - among exporters (and other suppliers such as original equipment manufacturers (OEMs)) and with access to sensitive items - of the risks associated with nuclear and nuclear-related goods, material, technology, software and expertise. While such sensitive items and skills are usually used for civilian purposes, they could also be misused in nuclear weapons programmes or terrorist activities. It is equally important to raise awareness of the danger that entities from countries suspected of proliferation might seek to obtain knowledge, know-how and access expertise that could contribute to a nuclear weapons programme.

Vigilance is required in the case of countries suspected of being engaged in the development or production of nuclear weapons. Such countries may seek to procure sensitive items or components directly or procure them via third countries.

No reputable company or organisation wishes to be involved in the misuse of any goods it produces or supplies. This policy is not just a matter of needing to comply with export controls but also in its own self-interest and corporate responsibility. Responsible corporate export control and due diligence means that organisations should assess transactions based on plausibility around things such as:

- no inconsistencies or lack of information provided by the potential recipient or customer;
- the plausibility of the stated end-use, and the item is appropriate in terms of its technical characteristics for that end-use; and
- corporate information given on the recipient/end-user statement is consistent with the stated end-use and is credible given all other circumstances (e.g. availability of the required expertise, technical and economic utility, order documents, end-use certificates).

III. Awareness-raising strategies

This document is only one of many ways of informing exporting organisations about the risks associated with supplying sensitive items that might be diverted for nuclear weapon activities. The inclusion of a “catch-all” provision in the NSG Guidelines has greatly enhanced the significance of corporate knowledge about the intended end-use and end-users of all items, not just those sensitive items that are listed.

The lists of controlled sensitive items drawn up by the NSG and regularly reviewed by the NSG Technical Experts Group (TEG) are a vital aspect of export control in the nuclear field. Under national and supranational legislation to implement this regime, the export of listed items usually is subject to some form of export licensing approval by a national authority. The precise details of the export licencing requirement are laid down in the national legislation of participating governments.

The parameters detailed in Section B below for determining the legitimacy of export transactions may be a useful toolkit for an organisation involved in exports or transfers, including whether there is a need for further information.. The most relevant of the specific parameters depends on the type of exporting organisation and the items or transaction involved. Experience has generally shown that such organisations should appoint one person to have overall responsibility at the senior management level and an additional contact person with whom the export licensing authority can liaise.

Since the relevant parameters will vary case-to-case, organisations should plan and adapt their export control processes accordingly. The examples of suspicious circumstances or behaviours are given in the sections below, these 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

The following parameters are intended to help organisations assess whether there is any risk of becoming inadvertently involved in nuclear weapons-related proliferation and whether they should seek further advice

I. Attempts involving nuclear and nuclear-related goods, material, facilities and Technology

Anyone involved in the export or transfer of nuclear and nuclear-related equipment, materials, software, and technology has to minimise the risks of unwittingly or unintentionally assisting in developing or producing nuclear weapons or nuclear explosive devices. Hence, special vigilance is needed to detect and prevent illicit procurement, with attention paid to any suspicious behaviour or business transactions relating to such items' supply.

Examples of suspicious behaviour that is inconsistent with standard business practice, include:

a) Inquiries received from previously unknown customers whose identity is not clear, who respond reluctantly to any questions regarding their identity or connections and where the answers may be evasive or unconvincing.

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

c) They are unable or reluctant to provide details of other commercial entities with whom they have previously dealt.

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

e) The customer is vague, evasive or does not provide clear, timely answers to:
   - questions about the intended use, end-user, facilities or details of the site where a component or equipment is to be installed; or
   - commercial or technical questions, which are typically part of any business contract negotiations.

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

g) The customer splits up a contract for plant construction or conversion without providing any adequate information about the full scope of the order and/or the final destination of the plant.

h) The customer requests completion of a partially completed project or installation of equipment that a different company has started without a credible explanation of why that company did not complete the work. The supplier may want to contact the initial company to confirm any explanation that is given.

i) The country of destination is suspected of being engaged in the proliferation of sensitive nuclear technology or seeking to acquire nuclear weapons, including through diversion activities.

Suspicious orders:

a) The stated destination or end-user for the items are unusual or implausible given the nature of the items to be supplied.

b) The declared value of the goods is inconsistent with standard business practice

c) The order itself is unusual in some way (e.g., the quantity or required performance of any spare parts significantly exceeds or falls short of the quantity or performance generally required for the stated end-use).

d) The description of the item to be supplied is vague or meaningless, or the specification requirements for the item are unnecessarily high given the stated end-use..

e) Equipment in an existing or planned facility is to be modified in a manner that would significantly change its performance characteristic, which could potentially help facilitate nuclear weapons-related development or production.

f) The site at which the equipment is to be installed is unusual given the nature of the facility and/or the stated end-use of the instillation.

Suspicious circumstances regarding the business environment:

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

b) The consignee or broker is deviating from their usual line of business or has recently been established, and therefore lacks a verifiable track record of work in the relevant areas.

c) The export supporting documentation does not match the information provided by the consignee or contains discrepancies in the description or quantity of goods to be supplied, or they are not of a standard usually expected for commercial transactions. Such as not being in the traditional format, containing spelling errors or other simple mistakes.

d) The customer requests unusual shipping or labelling arrangements, including packaging or part-packaging thereof, which would be inconsistent with the type of transport envisaged or the stated final destination.

e) The requirement for any special or unusual packaging and handling arrangements that do not match the stated use and/or final destination of the materials or components to be supplied, or similar suspicious arrangements.

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

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

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

The proliferation risk associated with the transfer of technical information, knowledge and know-how is generally even more of a concern than the export of physical items. This is especially true in the case of Intangible Technology Transfers such as by electronic means. Under the NSG Control Lists, sensitive information and know-how are termed “technology”. “Technology” is defined as consisting of both “technical data” (e.g., information) and “technical assistance” (e.g., know-how).

Proliferators can misuse scientific cooperation to acquire technology used to develop and produce nuclear weapons. There is a risk that allowing unrestricted access to universities and other scientific and technical institutions by scientists, research students and technicians from those countries engaged in proliferation enables them to acquire relevant advanced technologies. The knowledge thus obtained may be used not only for civil programmes but diverted to nuclear weapons-related activities as well.

The transfer of technology 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 and activities are also an opportunity to establish informal networks and contacts that enable expertise to be obtained on an ongoing basis that does not necessarily arouse suspicion.

Knowledge and know-how transfer can occur during the commercial, scientific and academic exchanges. Professional associations, technology centres and private and cultural initiatives also offer plentiful opportunities for potential proliferators to develop contacts and information-sharing. Another way of obtaining specific expertise is to directly approach experts and/or technical personnel involved, e.g., in the assembly or maintenance of production facilities.

Information transfer, in some form, is something that happens in every area of science and technology. The following parameters may help assess whether the expertise being sought might be used for nuclear weapons activities. 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 practices, for example, includes:

a) The lack of any request for expert technical 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 nuclear and nuclear-related goods:
   - inquiries from nationals of countries of proliferation concern about enrolling as a student, technical staff, or researcher on research projects;
   - requests to attend training courses, conferences and seminars from nationals of countries of concern; and
   - 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, researchers, and laboratory staff would not normally be expected to seek advice or information. The reasons for interest do not make complete technical sense or where evasive explanations are given.

e) The failure:
   - to explain or give convincing reasons why the technical data or know-how transfer and training is being sought;
   - to present or provide convincing answers to questions regarding relevant commercial or technical aspects of a contract; and/or
   - to demonstrate that the requesting party possesses the expertise typically required for any given projects.

f) Confidentiality or secrecy arrangements, which appear to be excessive **given** the nature of the services to be provided, or equally which demonstrate that the requesting party is clearly unfamiliar with the usual security requirements for such activities.

III. "Catch-All" controlling other items of proliferation concern

The development and production of nuclear weapons, or nuclear explosive devices, require the use and access to a wide range of general engineering or technical equipment, tools, component parts or materials. It would be impossible, and wholly impractical, to introduce specific export controls on all of the items needed for activities of proliferation concern. So to address this issue controls based on the end-use and end-user are often employed. These controls are termed "catch- all controls".

The guidance provided in this document can also be applied to the supply of these non-listed, more generic items, regarding generally awareness and specific things to look out for. Manufacturers and suppliers that have suspicions or concerns should contact the relevant national export licencing authority, who will provide advice.

The inclusion of a “catch-all” provision in the NSG Guidelines in 2004 established the need for relevant controls on the export or transfer of non-listed items which may, in part or in their entirety, be intended for use in nuclear-related activities of concern. To facilitate the effective implementation of "catch-all" controls, potential exporters need to be in a position to notify the relevant authorities of any suspicions that they have been approached to supply items destined for activities of concern. Since information about any suspicions is clearly crucial, exporters are encouraged to investigate within their capacity the facts of the matter before any export or transfer takes place. If their suspicions are confirmed or remain unaddressed, then they should notify the licensing authority accordingly.

IV. Attempts linked to nuclear terrorism

United Nations Security Council Resolution (UNSCR) 1540 was adopted in 2004 and is intended to limit the access by non-state actors (specifically terrorist groups) to weapons of mass destruction and the means of their delivery. UNSCR 1540 is in addition to resolutions that impose more specific measures aimed at combating terrorist activities by certain named persons and organisations.

UNSCR1540 mandates that States shall refrain from providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes. The resolution requires all governments to adopt and enforce appropriate laws to this effect, including export controls and other effective measures to prevent access to these weapons and their means of delivery by non-state actors.

In addition to the parameters listed in Sections I and II regarding exports and “technology” transfer, organisations should be aware of certain factors of specific relevance to preventing access by non-state actors and take appropriate action.

Manufacturers and suppliers should seek to know, to the greatest extent possible, their customers before entering contractual arrangements for the supply of materials, equipment or other sensitive items that could be used in the development or production of WMD or acts of nuclear terrorism

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 photocopied;

- the only means of contacting the party is via personal email address, a post office box or mobile phone number;
- the information provided about transport routes makes no geographical or economic sense;
- the party is clearly not familiar with (or ignores) security arrangements that are generally required or technically necessary for the handling or transport of nuclear and nuclear related goods; and
- the party clearly lacks the know-how or facilities necessary or recommended for secure storage or use, especially in the field of highly sensitive technologies or technical processes.

C. Information / National Authorities Contact Points

The NSG homepage: www.nuclearsuppliersgroup.org also contains links to the contact information of many of the NSG participating governments' national export-control authorities.

The NSG Guidelines with their lists of sensitive items (Control Lists) can be found in the NSG Guideline section of the NSG website:

https://www.nuclearsuppliersgroup.org/en/guidelines

Please contact the relevant national official body responsible for export controls in case of any doubt or questions concerning this document.