Good Practices for Implementing Controls on Intangible Transfers of NSG-Controlled Technology (ITT)

July 2025

Table of Contents

Introduction

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.

With increasing digitalisation on every production level, the transfer of technology is considered a growing proliferation risk, as it provides know-how to expand and refine research, development and production capabilities in sensitive areas.

In addition, transfers of relevant technology can be carried out by non-physical means (Intangible Technology Transfer - ITT). This includes transfers via electronic media (email, cloud services, etc.) as well as via verbal communication among experts/business partners. Extensive developments in communication technology and increasing international travel are constantly changing parameters in this environment. Those unique characteristics pose difficulties for export control authorities and exporting entities.

Due to the intangible nature of such transfers, traditional border controls are futile. At the same time, exporters must be highly attentive towards current regulations to prevent committing unintentional illegal acts. They have to identify and keep track of relevant ITT cases within their organisation, in accordance with export authorisation requirements and prohibitions. This is a great challenge for industry but also for research institutions and academia. Hence, national export control authorities are raising awareness in this field and are encouraging exporting entities to develop and practise effective due diligence.

Preventing unauthorised ITT requires partnership between authorities and industry or academia.

Industry and academia play an important role in controlling ITT. They are usually the first to become aware of possible procurement activities or new technological developments and can thus provide valuable insights into what proliferators may be seeking. ITT controls therefore are not a purely governmental task, but a joint task of government and industry or academia that requires close cooperation and partnership.

This document presents good practices on how to implement effective controls on intangible transfers of NSG-controlled technology. For the purpose of the application of suitable controls on intangible transfer of controlled technology, this guide provides an overview of the practices and considerations limiting unlicensed transfer of sensitive technology.

I. Control of Intangible Technology Transfer under the NSG Guidelines Part 1 and Part 2

The TECHNOLOGY CONTROL sections in the NSG Guidelines Part 1 and Part 2 provide that the transfer of technology directly associated with any item in the List will be subject to as great a degree of scrutiny and control as will the item itself, to the extent permitted by national legislation.

1. What does the term technology mean?

The term technology is defined as "specific information required for the development, production or use of any item contained in the List. This information may take the form of technical data or technical assistance."[1] Technical data may take forms such as blueprints, plans, diagrams, models, formulae, engineering designs and specifications, manuals and instructions written and recorded on other media or devices such as a disk, tape, read-only memories, or cloud services. Technical assistance may take forms such as: instruction, skills, training, working knowledge, consulting services.[2]

Technology

Specific information required for the development, production or use of any item contained in the List.

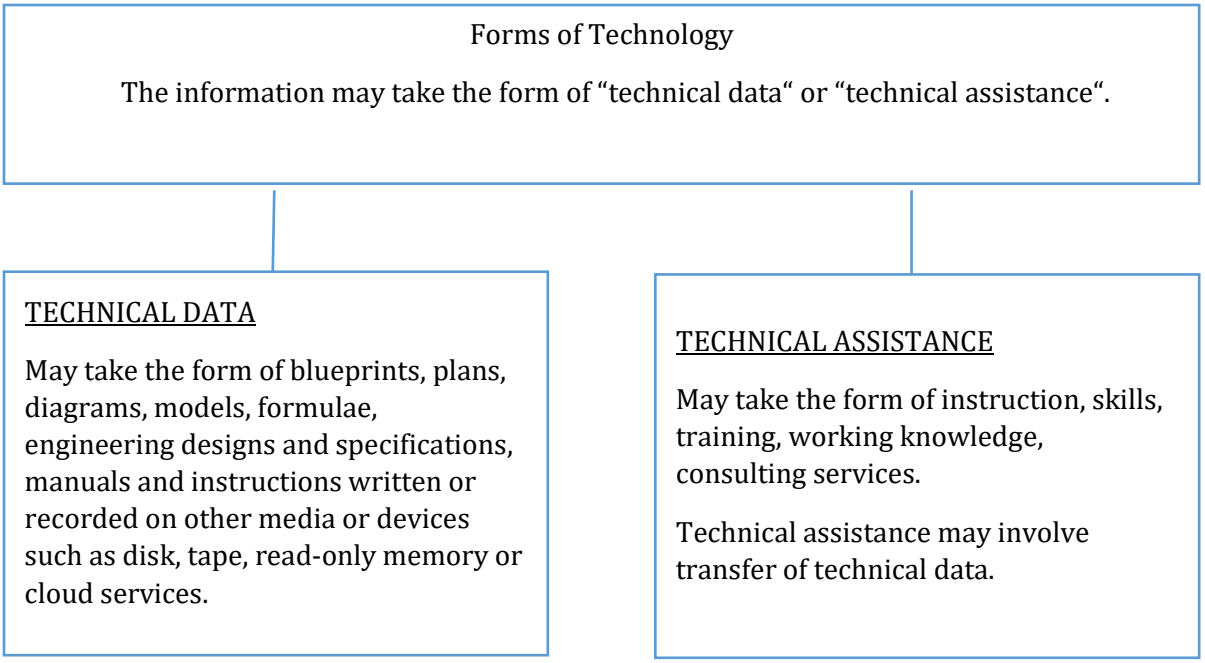
Development – is related to all phases before "production, such as: design, design research, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

Production – means all production phases such as: construction, production engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

Use – Operation, installation (including on-site installation), maintenance (checking), repair, overhaul or refurbishing.

[1] INFCIRC /254/Rev.14/Part 1, Annex A, Trigger List Referred to in Guidelines, Definitions; INFCIRC/254/Rev.12/Part 2, Annex, List of Nuclear-related Dual-use equipment, materials, software, and relate technology, Definitions.

[2] INFCIRC /254/Rev.14/Part 1, Annex A, Trigger List Referred to in Guidelines, Definitions; INFCIRC/254/Rev.12/Part 2, Annex, List of Nuclear-related Dual-use equipment, materials, software, and relate technology, Definitions.



2. What is not subject to control?

The TECHNOLOGY CONTROLS section in the NSG Guidelines Part 1 and Part 2 limit the coverage of the controls by specifying that they do not apply to information in the public domain and to basic scientific research.

a) Information in the public domain

Technology in the public domain is not subject to licensing requirements. Because once technology is available to everybody, export controls can no longer help prevent the technology from falling into the wrong hands.

The exemption stipulated in the TECHNOLOGY CONTROLS section refers to "technology or software that has been made available without restrictions upon its further dissemination. Copyright restrictions do not remove technology from being in the public domain."[3] The same applies for technology that can only be viewed after prior registration, as long as the registration is available without restriction to any individual who desires to obtain the information. Having to pay to view the information is also not a relevant restriction.

For exporters, and especially for academia, it is important to note that technology that is intended to be published is not yet in the public domain and therefore subject to export controls if no other exemption applies. It is also worth noting that technology derived from publicly available sources or methods is not necessarily in the public domain itself. In general, novel technological research will not be public domain, as it represents an addition to the total of what is known.

[3]INFCIRC /254/Rev.14/Part 1, Annex A, Trigger List Referred to in Guidelines, Definitions; INFCIRC/254/Rev.12/Part 2, Annex, List of Nuclear-related Dual-use equipment, materials, software, and relate technology, Definitions.

Technology may be made available to the public by any of the following means

- Provision in libraries available to the public
- Unlimited distribution at a conference, meeting, seminar, trade show or exhibition that is generally accessible to the interested public
- Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the internet on sites available to the public
- Publication by a patent office.

b) Basic scientific research

According to the TECHNOLOGY CONTROLS sections in the NSG Guidelines Part 1 and Part 2, basic scientific research is also not subject to controls. Basic scientific research is defined as follows in the Annex: "Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective."[4] It needs to be distinguished from applied research. This distinction requires an overall assessment of different criteria.

Criteria that may indicate applied research include:

- Research funding, or sponsorship by industry
- Directed at analysing, developing, producing or improving products through to market maturity
- Classified research
- Technology Readiness Level above 3.

For academia, it is important to note that there might be a gap between what some academics may consider "basic scientific research" and what the law actually considers to be "basic scientific research". Determining whether or not research activities fall within "basic scientific research" therefore is a process that requires close scrutiny and collaboration between export licensing officials, technical reach-back personnel as well as research and academic institutions.

[4] INFCIRC /254/Rev.14/Part 1, Annex A, Trigger List Referred to in Guidelines, Definitions; INFCIRC/254/Rev.12/Part 2, Annex, List of Nuclear-related Dual-use equipment, materials, software, and relate technology, Definitions.

Researchers engaged in research projects that were initially considered to be basic scientific research should repeat their assessment at different stages of the project in order to re-examine whether this assessment is still valid. The result of research may not always be foreseeable in detail; projects that are considered to be basic scientific research at the beginning may (even unintentionally) lead to results that are allocated to applied research. Those results would not be exempted from export controls.

Technology Readiness Levels

To distinguish between basic and applied research, some authorities suggest the use of so called Technology Readiness Levels (TRLs) as one criterion to be considered in the overall assessment.

TRLs are a type of measurement originally developed by the National Aeronautics and Space Agency (NASA) – not as an export control tool, but to assess the maturity level of a particular technology during the acquisition phase of a program. There are nine technology readiness levels that can be divided into four categories. While some countries tend to regard technology of the levels 1 to 3 as basic scientific research, others tend to consider only Level 1 and Level 2 technology as basic science research.

Basic Scientific		**TRL 1** – Basic principles observed **TRL 2** – Technology concept formulated
	Applied Research	**TRL 3** – Experimental proof of concept
		TRL 4 – Technology validated in lab **TRL 5** – Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
	Development	**TRL 6** – Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies) **TRL 7** – System prototype demonstration in operational environment **TRL 8** – System complete and qualified
	Implemen-tation	**TRL 9** – Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies, or in space)

Please note that the levels shown above correspond to those used in the EU. They slightly differ from the current NASA scale.

3. What does the term software mean?

The tern software is defined as a collection of one or more programs or microprograms fixed in any tangible medium of expression.

Software

"Software" means a collection of one or more "programs" or 'microprograms' fixed in any tangible medium of expression.

"Program" means a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer.

Programs therefore include source code files, written in a programming language, object code files and executable files.

"Microprogram" - A sequence of elementary instructions maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register.

A microprogram is a set of hardware specific instructions stored in special memory within a processor or other hardware component. Microprograms are commonly used in embedded systems and firmware.

4. Catch all Controls

The development and production of nuclear weapons, or nuclear explosive devices, requires 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.

The NSG Part 2 Guidelines[5] therefore provide that Nuclear Supplier Countries should ensure that their national legislation requires an authorisation for the transfer of items not listed in the Dual-Use Annex if the items in question are or may be intended, in their entirety or in part, for use in “nuclear explosive activity”. Accordingly, Participating Governments often employ controls based on the end-use and end-user. These Controls are termed “catch-all controls”.

Catch-all controls may apply to all types of non-listed items that are objectively technically suitable for use in connection with a nuclear explosive activity. They are often relevant for items that are similar to “listed” items but that fall (just) below the technical specifications threshold for “listed items”, as proliferators actively seek to procure non-listed items that can be used as a substitute for more stringently controlled listed items. However, procurement attempts may also involve non-listed items that are necessary or usable for the production of NSG-relevant items.

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,

[5] INFCIRC/254/Rev.12/Part 2.

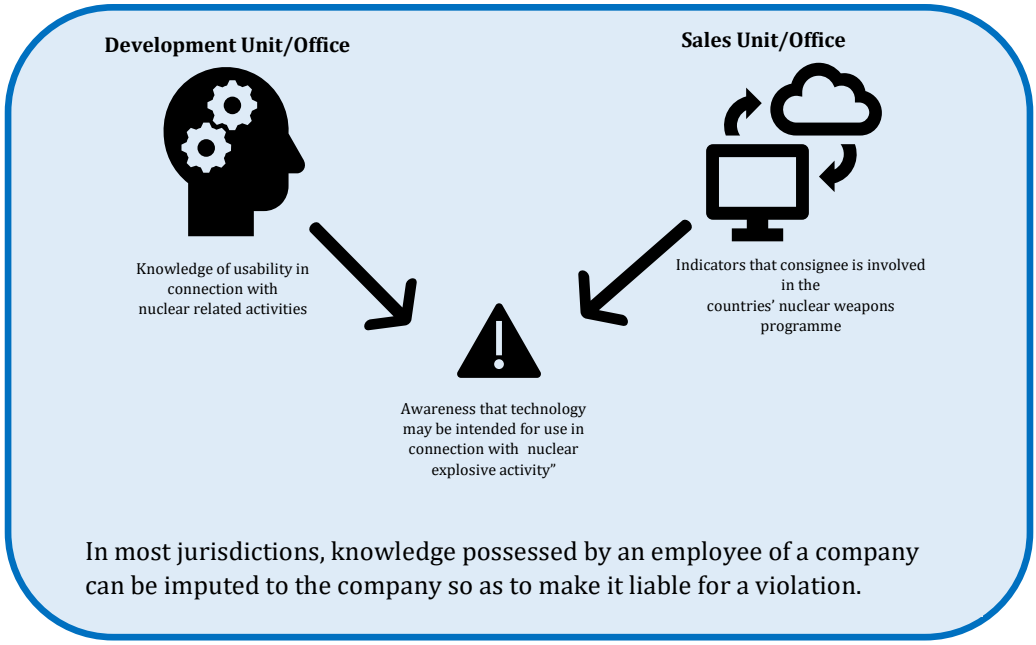
exporters are encouraged to investigate within their capacity the facts of the matter before any export or transfer takes place. If their suspicions are confirmed or remain unaddressed, then they should notify the licensing authority accordingly.

To be able to identify possible procurement attempts, industry and academia should understand the capabilities and potential applications of their technologies for nuclear explosive activity and should familiarise themselves with the market (suppliers and buyers) of their products or, in the case of researchers and scientists, with the actors in their research field. A profound understanding of the market or research landscape will allow them to determine whether the nature and scale of the technology correspond with the type and technological sophistication of the consignee's business or research and the country of destination.

If the company becomes aware of a sensitive end-use, the competent authority must be notified. Suspicion alone does not trigger the obligation to notify, but exporters should be vigilant for signs of suspicious enquiries or orders ("red flags"). They have a duty to check out suspicious circumstances. The transaction should take place only if the suspicious circumstances can be explained or justified. Otherwise the authorities should be informed and it must be ensured that no export occurs without a final decision having been taken by the authority.

Bearing this in mind, exporters have to ensure that information about an ITT all comes together at one point in the organisation and can be taken into account by the export control personnel when assessing whether the company "is aware" of an inappropriate end-use. This requires clear reporting obligations to the export control personnel, e.g. by the development and sales department.

For cases in which the company is being informed by the competent authority, a procedure must be in place to ensure that information is forwarded to the export control personnel and that the transfer of the non-listed technology will be stopped immediately.



5. How is Technology Intangibly Transferred?

The NSG Guidelines provide for two distinct situations in which an intangible transfer could occur:

- First, the transmission of NSG-controlled technical data by electronic media (email, cloud, the internet, the intranet etc.), fax or telephone. In this case, the technology is fixed in a tangible medium (hardware such as read-only memories, disks, memory cards, servers etc) before and after the transfer. The means of transfer, however, is intangible.

- Second, the transfer of knowledge as technical assistance may be conducted verbally from one person to another (e.g., in conversations, discussions, meetings, conferences) or manually through the provision of technical services. In this case, both the technology itself and the means of transfer are intangible.

Tangible technical data or software		**Intangible technology or software**
Tangible transfers	**Intangible transfers**	**Intangible transfers (Technical Assistance)**
- post - hand carried on an electronic storage medium or paper	- email - email attachments - fax - the internet, via download - "cloud" sharing - Updates or upgrades - troubleshooting	- instructions - skill training - technical services - academic courses, such as PhD programmes in certain disciplines - presentations - seminars - conversations and discussions - briefings - web conferences - meetings - workplace collaboration - job shadowing

II. Control of Software Transfer under the NSG Guidelines Part 1 and Part 2

The SOFTWARE CONTROL sections in the NSG Guidelines Part 1 and Part 2 provide that the transfer of software especially designed or prepared for the "development", "production" or "use" of any item in the List will be subject to as great a degree of scrutiny and controls as will the item itself, to the extent permitted by national legislation. For the purposes of implementation of the Guidelines for "software" transfers, suppliers should apply the same principles as for "technology" transfers.

III. Implementation Strategy

1. Export Licensing

The multilateral export control regimes (including the NSG) apply controls to the transfer of technology associated with any regime-controlled item. These technology controls apply when the technology is transferred by tangible or intangible means. As a result, ITT is subject to licensing requirements. As with all NSG-controlled items, these requirements are not export bans but rather a requirement for governments to consider the appropriateness of each export on a case-by-case basis.

Note:

- Intra-company and intra-group transfers or releases may also be subject to export controls.

The implementation of these ITT controls falls within the responsibility of the NSG Participating Governments. Therefore, the way in which the controls are implemented in national law varies among PGs.

a) Activities subject to licensing requirements

However, ITT subject to licensing requirements may include the following activities:

- **ITT across national boundary out of the country**.

  The transmission of controlled technology across national boundaries out of the country constitutes an export and is therefore subject to control – even if the transmission is only temporary.

  NSG Participating Governments usually also control the cross-border release or making available of technology to persons outside of the originating country. The controls might either concern the actual access by the person abroad or the preceding act of providing (potential) access. In the latter case, it is not necessary that the person abroad actually access or download the technology that is made available.

- **ITT to a foreign person within the originating territory**

  In some NSG Participating Countries, the transfer or release to a foreign person within the originating territory is deemed to be an export to the foreign person's country of origin ("deemed export"). Other NSG Participating Governments consider these ITT as technical assistance[6] that is made subject to license only if it is or may be intended for an inappropriate use, such as in nuclear-related activities of concern. In both cases, it is essential that organisations hosting foreign visitors are aware of the relevant export control requirements and free to consult with export licensing officials before such visits occur.

- **ITT to a foreign person while in a foreign country**

  The transfer or release of controlled technology to a foreign person while in a foreign country may – depending on the national jurisdiction – be deemed to be a (re-)export to the foreign person's country of origin and/or considered technical assistance.

[6] In some Participating Countries, the term technical assistance is used not only to describe the form of controlled technology, but also to describe an activity subject to controls that differs from exports mainly in how the technology is transferred.

b) Challenges in implementing export controls in selected business processes and in the academic sector

The licensing requirements for ITT may be relevant for a variety of activities in an organisation. These include, for example, ITT via Cloud Computing and ITT in connection with business trips.

(1) Cloud Computing

ITT may also be conducted via cloud computing.

There is no generally applicable definition of cloud computing but, simply put, cloud computing is the delivery of computing services – including storage, databases, networking, software, analytics and intelligence – via the internet ("the cloud"). There are three main types of cloud computing: software as a service, platform as a service and infrastructure as a service.

Software as a Service (SaaS)	SaaS is the delivery of single applications, such as email services, in the cloud.
Platform as a Service (PaaS)	In PaaS models, cloud providers deliver a computing platform application developers can use to develop and run their own software.
Infrastructure as a Service (IaaS)	IaaS is a computing infrastructure, provisioned and managed over the internet.

When using cloud services, industry and academia have to ensure they comply with the restrictions for ITT. The activities that may be subject to license include:

- Storage of controlled technology or software if all or part of the cloud provider's servers are located in another country than the country of origin.
  However, some Participating Governments allow their companies to use cloud technology to transfer and store controlled technology and software subject to controls without facing export control licensing requirements – as long as the transfers and storage meet certain provisions, inter alia with regard to encryption.

- Storage of controlled technology or software in a cloud the servers of which are located in the country of origin if foreign persons or persons abroad access the technology or are in a position to do so.

The storage of export-controlled technology on a third-party server creates the risk for unauthorised access at the physical location of the servers or among those individuals that administer the network. Therefore, Participating Governments usually require, or at least call for, security measures to protect controlled technology against unauthorised access. The security measures to be fulfilled are either explicitly defined or the licensing authority refers to state-of-the-art and good practices in this field.

Criteria that may be taken into account and that play a role in whether or not a license is required and can be issued include:

- Is the technology classified?
- Where are the servers of the cloud physically located?
- Where are the individuals that administer the network, and what rights do they have?
- What access options do government agencies have due to the (foreign) jurisdiction that applies to the cloud provider?
- Is the intent to make data on cloud servers available solely for internal use? If not, how will external access and foreign access be controlled?
- How is access granted and does the administrator keep detailed records of user access, including physical location?
- Is the information encrypted for storage and transmission?

(2) Remote Work /Mobile working

Organisations must have procedures and controls in place to identify export licensing requirements and prohibitions that might apply in connection with international business trips. Some Participating Governments consider the temporary carrying of controlled technology or the access to such technology during a business trip as an export subject to license requirements.

If so, Notebooks or any other hardware that employees want to take on a business trip abroad must be screened for possible export-controlled technical information stored on the device or accessible via the device. In cases where it is not practical to determine whether the employee's device contains controlled data or software, organisations may encourage employees to travel with a device that only contains the standard set of pre-loaded software that has been approved by an organisation's export control personnel. The upload of any additional data or software should only be possible with the approval of the export control personnel.

Exporters should also be aware that the export control law of the country of destination has to be observed when leaving the country with controlled technology in one's luggage.

(3) Marketing Activity

Licensing officials should be sensitive to the prospect that unauthorized ITT may occur in advance of conventional export activity and before an export license would normally come to the licensing

authority's attention. Unauthorized ITT may occur because some types of marketing, business development, or sales consultation activity could involve the transmission of controlled technology with unauthorized parties. In such cases, the transmission may occur over the telephone, via email exchanges, during a foreign national visit to the manufacturer, during a company representative's travels overseas, at trade shows, etc

(4) Academia

The implementation of ITT controls in the academic sector can be challenging. As, in many countries, the freedom of research is a constitutionally guaranteed right, members of the academic community are often used to freely pursuing, developing and transmitting knowledge and ideas through research, teaching, study, discussion, documentation, production, creation and writing. However, export controls may apply and need to be considered, without discouraging the exchange of academic ideas essential to international scientific and educational cooperation, but promoting a trustful academic cooperation secured via compliance with export controls.

The transfer of technology may occur through national and international conferences, workshops, meetings, symposia, joint research and development projects, as well as training and education programmes or by allowing unrestricted access to universities and other scientific and technical institutions by scientists, research students and technicians. Members of the academic community should therefore be aware of the principles of non-proliferation. The knowledge obtained through scientific cooperation may be used not only for civil programmes but may be diverted to nuclear weapons-related activities as well.

When implementing ITT controls, the academic sector and subsequently export control authorities face distinct challenges, such as:

- Organisational structures: Unlike companies, many academic and research institutions are not organised in a strict hierarchical manner making it at times more difficult to implement certain policies and rules top-down;
- Publications are intrinsic to academia: the goal of research is to publish the research results, in academic journals, at conferences etc.;
- Scientific exchange is international: institutions work in international research networks, teams operate cross-border, research exchanges happen worldwide;
- Research often pursues a general interest: researchers often aim for improvements, e.g. in public health, communication, infrastructure etc. and weigh it against the potential misuse; they are often familiar with ethical issues but less with export control;
- Researchers often operate with the assistance of public funding thereby at times being under the requirement to make the research results available to the public;
- Often researchers are at the forefront of new technological developments that might not be subject to export control items lists yet.

c) Addressing ITT Concerns in an Export License Assessment and Limiting the Risk of unauthorized ITT

One of the primary licensing challenges with ITT is determining when there is an ITT risk and issuing license determinations that mitigate such risks. The use of license conditions (or restrictions) is a valuable way to mitigate potential ITT risks.

For export license applications involving a „technology transfer", it can be helpful for government officials to require supplemental information, including

- Identities of all parties
- Specific role of foreign national(s)
- Exact project location where the technology will be used
- Type of technology or software
- Form in which the technology will be released
- Use for which the data or software will be employed

Within the context of ITT, license conditions typically fall into the following broad categories:

- Clearly specifying what is and is not approved in terms of technology transfer (e.g., "No discussion or transfer of source code or system performance parameters used for modelling")
- Limiting access to approved technology to a defined set of personnel (e.g., "No transfer of technical data to Third Country Nationals")
- Requiring data protection, access control, and record keeping (e.g., "Transfer of manufacturing specifications, tolerance, and testing procedures must be solely within the company's encrypted IT system and access limited to approved end users")

There are several additional issues related to export licensing and ITT that may factor in to an export license determination. National laws, regulations, and export licensing procedures should consider many of these unique issues and ensure adequate government oversight is provided in all instances. The following list provides examples of common export control-related issues that may be especially relevant to transfers of technology in general, and ITT in particular.

Access Control: Commodity exports, particularly for manufacturing and test equipment, often have accompanying controlled technical data and/or technical assistance. Some end user facilities may have individuals present *(e.g.,* third country nationals or visitors from other companies) who could gain access to controlled technology through physical inspection of the equipment, and should not be allowed to access to the equipment or controlled technology.

End-use verifications: Officials may also consider adding extra requirements or license conditions to permit end-use verifications *(i.e.,* pre-license checks and post-shipment checks) on equipment after it has been exported and received by end users. These checks may be conducted with an eye towards ensuring equipment is stored in a secure physical- and cyber-environment so that unauthorized end users cannot gain access physically, visually, or electronically. Some entities, especially those involved

in research and development, may conduct operations using common networks, which may add to the risk of unauthorized access.

Data Encryption: In some countries, export control regulations allow information and software to be sent from one location to another without an export license if there is "end-to-end encryption" that prevents an unauthorized foreign national from accessing the information. As an added assurance, some Participating Governments prohibit hosting internet servers or databases with export -sensitive information in countries that lack sufficient strategic trade controls and security.

Limiting the transfer of "know-how": In some cases, licensing officials may permit the export of a certain item, but not allow the export of "know how" associated with the inner working of the item. This can be accomplished in a variety of ways, such as requiring all maintenance and refurbishment occur at the original manufacturer (rather than in the end-use country) or preventing the transfer of software source code. Additional areas to consider include limiting the transfer of design rationale, manufacturing and design know-how, and troubleshooting. In many cases, licensing officers should attempt to limit the transmission of technology only to what is needed. For example, training that accompanies the export of certain equipment should be limited to only that which is required to operate that equipment in its intended role, and not for training on design technology, advanced troubleshooting, modifications, upgrades, etc.

Manufacturing License Agreements / Technical Assistance Agreement: Certain activities subject to export controls may carry a higher risk of unauthorized technology transfer in general and ITT in particular. These business-related activities include manufacturing operations in a foreign country, technical consulting and advising services, and joint ventures. Export license officials may benefit from generating distinct export license application processes and procedures for these types of activities to better address specific risks. A Manufacturing Licensing Agreement (MLA} or a Technical Assistance Agreement (TAA) are examples of export licensing processes that ensure the government has a chance to fully review and assess a proposed activity for export control implications before any significant technical discussions occur.

Non-Disclosure Agreements and Proprietary Information: Many companies implement a range of legal measures and operational procedures to protect their own proprietary technology. The "technical know-how" behind a commodity or process is often the most valuable part of a company's product line and therefore something that is highly protected. Export licensing officials should consider seeking out information regarding an exporter's process for protecting business-proprietary information, including such mechanisms as non-disclosure agreements. This analysis may lead to a better understanding of potential risk-reducing factors in a proposed export. However, it would not be prudent to assume that a company's internal information protection processes are sufficient to address all export control concerns.

2. Enforcement

The transfer of knowledge as technical assistance through instruction as well as the transfer of technical data in a non-physical form present significant challenges to the enforcement of export controls traditionally based on national boundaries. Therefore, unique policies and practices for effective enforcement are required.

The following section outlines various enforcement strategies, which Participating Governments may find useful in this context:

a) Pre-transfer measures

Identifying proliferation-related ITT and information sharing:

A possible measure could be an increased international exchange among the competent control authorities to share information on suspicious attempts to acquire NSG controlled technology. If national law permits, control authorities could monitor specific entities to prevent illegal transfers of controlled technology.

Especially, when acquiring sensitive technology is the sole purpose of a proliferation effort and not linked with procurement efforts to acquire related physical commodities and equipment, it can be very challenging for authorities to identify and investigate those cases. Authorities should therefore consider the following tactics that proliferators may use to acquire sensitive information through ITT:

- Sending unsolicited emails to faculty and staff at industry/universities
- Using front companies in locations that may lack strong export controls and/or locations with access to proliferation-sensitive technologies via trade networks
- 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.
- Building liaisons with universities that have ties to defense contractors
- Recruiting of technical experts by foreign intelligence services
- Recruiting of technical experts to serve as ”advisors“ on government or industry projects
- Soliciting information from national laboratories or seeking to establish research relationships focused on dual-use technologies
- 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.
- Stealing electronic information by hacking/compromising laptops and other communication devices while travelling overseas
- Attending/hosting conferences and trade shows
- Relocating R&D facilities overseas to locations that receive less scrutiny or locations with domestic technical expertise
- Circumventing export control laws by smuggling or falsifying documents
- Visiting research and development or manufacturing facilities of potential ”supplier“ companies
- Joining scientific and research delegations

- Downloading unprotected, but potentially export-controlled, information from a university or company network
- Recruiting retired scientists
- In connection with nuclear and nuclear-related goods:
    - inquiries about enrolling as a student, technical staff, or researcher on research projects;
    - requests to attend training courses, conferences and seminars; and
    - requests from unknown individuals, institutions and companies for help and advice in a specific area of technology and/or technical process.

Visa Screening:

As to oral transfers of NSG-controlled technology[7] on national territory, the screening of visas may be a useful instrument for preventing proliferation.

Countries may seek to use existing visa screening procedures to prevent proliferation. One objective could be to establish whether there is any link between specific visa applications and certain sensitive nuclear weapons activities. Special care could be taken when screening visa applications from graduate students and scientists in sensitive disciplines. Visa-issuing authorities could require comprehensive information from applicants and apply a risk profile based on nationality or possible links to nuclear-related business and industry.

Authorities could be encouraged to exchange information on, and obtained through, currenct visa screening practices (trends, suspect, persons and institutions, etc).

b) Post-transfer measures

By its very nature, the electronic transmission of technology, e.g. by downloading data or sending faxes or e-mails abroad, creates considerable possibility for illegal transfers. That is why external audits to ensure compliance with export controls as well as criminal investigations to uncover illicit transfers are so important.

If all transfers that require licenses are documented, this facilitates audits and criminal investigations. Industry, academic institutions and individuals should be obliged to keep certain records of electronic transfers of controlled technology for an appropriate period of time (e.g. the last 3 years, in accordance with national legislation and practices. Adapting record-keeping requirements to the different types of licenses reduces the administrative burden on companies and institutions.

Whenever oral or manual transfers of controlled technology do not involve tangible sources of information, enforcing controls on the transfer as such and post-transfer monitoring becomes difficult. However, oral or manual transfers of controlled technology will often go hand in hand with tangible exports of controlled technology. Scientists, designers, engineers and other persons involved will take tangible sources of technology abroad to back up the transfer of personal know-how.

Both external auditing and investigation authorities require highly trained and specialised staff to develop auditing strategies and investigation techniques designed to detect illegal electronic transfers, e.g. by examining server protocols.

[7] This does not include information in the public domain or basic scientific research

Other documents that may provide evidence of illegal intangible transfers include:

- business documents,
- internal communication papers,
- financial transactions, and
- contacts with tangible information recipients prior to and after the respective transfer.

Possible elements of a comprehensive criminal investigation strategy include:

- examination of correspondence and telecommunications based on a strong indication that an illegal act has been committed; in this context fundamental and legal rights are to be respected;
- search warrants and confiscation of items;
- observation;
- exchange of data among public authorities;
- interviews;
- monitoring of financial transactions.

c) Intangible electronic transfers to foreign persons within national borders

In addition, some methods of regulating the electronic transfer of controlled technology within national borders should be considered, when the same transfer would require an export license if exported to the country of which the foreign person is a national.

IV. Recommendations for internal ITT Controls

Exporters play a pivotal role in achieving export control objectives. Export Controls can only be effective when all parties involved are aware of and comply with such controls. The fight against the proliferation of weapons of mass destruction requires maximum cooperation. Consequently, one key element to successful implementation of controls of intangible transfers of NSG-controlled technology is self-auditing by industry, academia and individuals. On the part of control authorities, this requires awareness-raising and outreach programmes to inform and involve industry and academia, and visits to measure “good practices” and compliance with export controls.

1. Awareness-raising strategies

By raising awareness amongst exporters for the risks associated with ITT as well as by providing expertise and advice to industry and academic institutions on how to design and implement internal compliance programmes, governments can help reduce the burden on their export control authorities. In most cases, companies and academic institutions also have an interest in ensuring that sensitive items are not inadvertently supplied for use in nuclear weapons activities – not to mention industry’s proprietary interest in denying sensitive information to competitors. The work of export control officers in industry and academic institutions is crucial in providing target groups with easy access to all relevant information and advice on ITT.

a) National Outreach to Industry

Many countries engage regularly with their industry and have established well-developed outreach programmes.

In order to effectively address the risks associated with ITT, these outreach efforts should seek to:

- Identify and highlight employee activities that may present ITT risks
- Promote company review and record keeping of technology transfers, including person-to-person interactions
- Promote information security "good practices" to prevent inadvertent or malicious access to controlled technology

b) National Outreach to Academia

As highlighted above[8], for universities and research organisations, compliance with ITT controls can prove to be challenging. Due to the academic freedom they enjoy, they are used to freely and independently pursuing, developing and transmitting knowledge and ideas through research, teaching, study, discussion, documentation, production, creation and writing. However, as non-proliferation and peaceful uses are mutually reinforcing, researchers, too, must comply with export controls to ensure a trustful and secure academic cooperation.

So to adequately address these challenges in a balanced manner, Participating Governments should provide regular training sessions to make researchers aware of the restrictions of foreign trade law, which may apply even if the research is intended for civilian purposes. In order to create understanding for the restrictions of foreign trade law, the training sessions should also address the objectives of export controls – without discouraging the exchange of academic ideas, which is essential to international scientific and educational cooperation. Furthermore, workflows should be set up that cover all forms of ITT in the organisation. The potential issues to be covered should include:

- Foreign students pursuing highly technical, nuclear related degrees
- Transfer of research results to persons abroad or foreign nationals via email or other electronic/data storage device
- Research instructions or skill training conducted for a foreign national
- Foreign student access to research lab equipment and techniques
- Research collaboration with foreign universities and foreign professors
- Overseas lectures and speaking engagements
- Foreign visiting professors
- Outside consultancy employment of professors

c) Conducting visits to measure "good practices" and compliance

Regular auditing of internal compliance programmes by export control authorities helps to promote "good practices" and to measure compliance with controls on electronic, oral and manual transfers of controlled technology. Entities should be required to demonstrate the effectiveness of their internal compliance programmes.

To do so, entities should:

- be familiar with export control legislation and precisely classify all the listed items they deal with;

[8] See Section III. 1. b) (5).

- have a system in place to ensure that all staff is aware of the export control issue and adhere to the required procedure for making a transfer of controlled technology;
- assign clear responsibilities for export controls (preferably involving senior staff) and
- have a system in place to ensure that licenses cover all relevant transfers of technology.

Export control authorities' awareness-raising and training efforts should focus on entities that are found to be significantly lacking in compliance.

2. Self-auditing by industry, academic research organisations and universities, individuals

The following is intended to assist exporters in complying with the restrictions on ITT. In order to comply with the restrictions for ITT, organisations have to identify and keep track of ITT in their businesses processes (a). Before an ITT is conducted, exporters must ensure that they know the recipient of the technology as well as the purpose for which the latter intends to use it (b). In accordance with the principles outlined above, the exporter must determine whether the ITT is subject to a licensing requirement. When submitting an application, the exporter has to ensure that complete information is provided and that the necessary documents are enclosed (c). Once a license has been issued, the exporter must ensure that the export to be made is within the scope of the license and that the terms and conditions of the license can be met (d).

a) Identifying and keeping track of ITT

Organisations should have processes in place that ensure knowledgeable export control personnel become aware of export-controlled intangible technology transfers at an early stage and can assess whether an export license must be obtained.

A key challenge for organisations is to identify and keep track of all cases in which transfers occur. ITT is not always tied to a specific commodity sale or export that is channelled through the sales

The export control personnel must have the authority within the organisation to stop any ITT, which would violate export control laws and regulations.

department, but may also be conducted, e.g., during direct interaction between technical experts of the development department, by IT experts moving data within the group or building a new infrastructure or during the initiation of a business relationship by marketing personnel.

Moreover, employees who have not been appropriately sensitised and trained are generally unaware that everyday activities such as sending an email or uploading data to a network may constitute an export requiring a license.

It is therefore important that all employees of the organisation who are potentially involved in transfers of controlled technology are trained and sensitised for export control restrictions on a regular basis. Especially for new employees, training must be provided.

Make sure that your potential customer is not on a sanction list applicable in your country.

b) Transaction screening

Before an ITT occurs, exporters are required to identify the customer and to exercise due diligence in order to determine/assess the risk that the technology to be exported will be used for an undesirable end use or diverted to an undesirable end user.

Exporters should ask the customer to provide minimum requirements for identification of the parties involved in the transaction and information on the intended end use of the technology. In addition, the exporter should collect all available data on the parties involved from trusted sources, e.g. online information or news reports.

In order to evaluate whether there is a legitimate need for the technology, ask for information on the intended end use and request an end-use certificate.

The information collected as well as the circumstances of the business relationship should be verified and scrutinised for any inconsistencies or "red flags". Red flags are abnormal circumstances in a transaction that indicate the export may be destined for an inappropriate end-use, end-user or destination. Included among examples of red flags are customers whose identity remains unclear or who are reluctant to provide information about the end-use of the product as well as orders that are inconsistent with the needs of the purchaser or requests for unusual shipping routes or payment methods.

Be vigilant for signs of suspicious enquires or orders!

As a business practice, exporters should review sales and marketing activities after a set period of time (e.g. quarterly, or semi-annually, annually) for any possible technology transfer involving missile-relevant items.

c) Applying for an ITT license

Before conducting an intangible transfer of controlled technology, exporters have to file an application with the competent authority. In some countries license applications must be made using an online licensing system, other PGs allow for applications to be sent by post.

The application should contain the classification number and detailed technical specifications on the technology.

In addition, the exporter is usually required to indicate the quantity and value of the item to be exported. However, in case of ITT, the exporter may not always be able to provide this information. Therefore, when it comes to reporting a quantity, Participating Governments usually allow exporters to either not complete the quantity box, as being not applicable in case of ITT; or, if the completion of the box is mandatory, to insert a nominal quantity. Regarding the declaration of value the competent authorities usually do not object if exporters either make a best judgement or again enter a nominal number like "0" or "1".

Finally, the exporter may also be asked to illustrate the security measures he will take to protect the technology against unauthorised access.

Together with the application the exporter is required to provide an end-user statement. Most Participating Governments provide a form for the statement. The statement has to be completed by the end-user, not the exporter or the intermediary/consignee on behalf of the end-user. Before the statement is submitted to the licensing authority, the exporter should review whether the document has been filled in completely, is readable and whether the stated end-use is reasonable.

d) Using a granted license

Upon receipt of the license the exporter should check the terms and limitations of the license.

The exporter has to ensure that only authorised technology is transferred. As a first step, the exporter must therefore gain a clear understanding of the scope of the authorised technology.

In addition, the exporter has to establish and maintain compliance with possible administrative requirements associated with the license. Export licenses usually do not restrict the means of transfer

Inform export control personnel about technology in the product portfolio that is technically suitable for use in connection with nuclear explosive activity.

but authorise the technology transfer in general by whatever means the parties deem appropriate. However, depending on the means of the transfer, the license may require specific security measures the exporter has to apply (e.g. requirements with regard to data protection). It may also limit the access to approved technology to a defined set of personnel. Also re-exports or retransfers may be restricted. In addition, the license may contain reporting or documentation requirements. The terms of the license may also require the exporter to get in contact with the recipient, e.g. to inform him about possible re-export restrictions.

It is also important to keep an eye on the validity of the licenses, to renew them on time and to avoid gaps between the licenses that might prevent the timely delivery of the technology. In some countries it is also advantageous from a procedural point of view to apply for an extension before the previous license has expired, as requests for renewal can then be decided through a simplified procedure.

V. Food for Thought: Proposals for a Regulatory Frame for implementing export controls on ITT via the Software as a Service model in Cloud Computing

Software as a Service (SaaS) is the delivery of single applications, such as email services, in the cloud.

The SaaS delivery model implies an infrastructure platform that hosts software applications that can be accessed on the web. The platform is usually represented by a public cloud that either may reside on the exporter's own data centre, or may be hosted by an independent PaaS provider.[9]

Licensing authorities could consider recommending that NSG-controlled software applications should be uploaded to a cloud in an encrypted format, with access only granted through credentials and security keys provided by the exporter. This assumes the exporter is also the software developer providing the cloud-based service.

Intangible transfer of NSG-controlled programs may be considered exports of software rather than technology, even if the final user cannot modify the transferred files. However, granting access to NSG-controlled programs in executable form, hosted in the cloud, may be considered an intangible transfer of technology.

It may be necessary to determine if an export license is required for the act of uploading the encrypted application files to a cloud, when they are inaccessible without access credentials, or if an export license is only required when access to the application is granted to the end user.

A transfer of files (technical data, operating instructions, programs etc.) from a cloud to the final user's computer following access to a software application hosted in the cloud may require a separate export license from the authority that also authorized access to the SaaS application.

For example, to allow a user to run the SaaS application, an exporter might need a license for export of technology described in category 1E in INFCIRC/254/Rev.12/Part 2 Annex. If the SaaS application generates a NSG-controlled program that the final user can download, the exporter might also require an export license for category 1D software.

The location of a user accessing an NSG-controlled SaaS application based on user-password credentials cannot always be determined. The application may be accessed from an internet-connected device, regardless of its physical location, which may differ from the authorized country of destination.

As a possible pre-transfer control, authorities might consider to request exporters to check the IP (Internet Protocol) address of the user via web service. Access could be restricted to IP addresses consistent with the country of destination specified in the export license. Alternatively, access could be limited to GPS-enabled devices, with verification that geolocation data matches the licensed country of destination. Access logs (including user ID, location, access date and time) could be requested to be recorded.

As a post-transfer measure, the licensing authority could be granted rights to access the hosting platform, read the access logs and verify license compliance as a condition for authorization.

A stricter approach might involve limiting access to a set of specific IP addresses to be listed in the license.

Further discussions could explore the ongoing evolution of internet and satellite communication technologies. For example, users may circumvent IP checks via VPN (Virtual Private Network) which masks the user's IP address by routing traffic through remote servers. As a countermeasure, software

[9] In PaaS models, cloud providers deliver a computing platform application developers can use to develop and run their own software.

and hardware products are increasingly available to detect and block VPN traffic. Similarly, GPS jammers can disrupt signal reception, although flickering location data typically reveals interference. Multiple detection checklists for GPS jamming are available.

As more and more data and information is transmitted over the internet, stronger technical controls could be identified and applied, even if some may seem excessive. Given the rapid evolution of telecommunication, technology should be closely followed, in order to implement more effective export controls and compliance mechanisms.