European Studies Unit

US Export Control Regulations Explained to the European Exporter: A Handbook

Rosa ROSANELLI

US Export Control Regulations Explained to the European Exporter: A Handbook

Rosa ROSANELLI

Contents

1. Introduction

In the era of intense global exchanges and fast, intangible transfers, international security is highly dependent on the ability to track and control the dissemination of particularly sensitive or potentially proliferating items.

The responsible management of trade passes through "export controls": international agreements, national laws and implementing regulations that serve each state's commitment to international peace and security, but also represent a critical tool of foreign policy and the protection of strategically important technology.

In this sense export restrictions find their most meaningful example in American regulations. For the world's largest producer and exporter of defence articles, services and technology, controlling their dissemination is crucial to protect national security and commercial interests, but also closely linked to its right to sovereign self-defence.

Pervasive, complicated and characterised by extraterritorial outreach, US export laws and implementing regulations place restrictions on broadly defined "exports" of sensitive items, software and technology and affect American and foreign entities alike.

It is therefore critical that these requirements are well known and thoroughly understood by the European exporter, especially in times when risk exposure tends to be extended to new actors. While businesses related to defence, aeronautics and space or energy services have been concerned about export control issues for years, there is a trend towards extending the scope of regulations to companies dealing with insurances, financial institutions, ITC, automotive industries, but also to public organisations and independent legal advisers.

This handbook is a useful tool for European operators. While nothing provided here can substitute for consulting the applicable legal texts, exporters might find guidance to be more aware of export restrictions, understand their rationale, find the answers to their questions, and better manage their compliance obligations.

2. Controlling exports in the US: the American perspective

The United States plays a fundamental role in global trade of defence and strategically sensitive goods. For the world's largest producer and exporter of defence articles, services and technology[1], controlling their dissemination is an imperative for the preservation of international and national security. But not only: export controls are also an important foreign policy tool, closely linked to the right to sovereign self-defence.

In drafting and reviewing export control laws and their implementing regulations, the US seems to abide by some fundamental principles such as:

- "**Transparency**": core to the US regulatory system, that systematically allows stakeholders to provide comments, not only in the US but from anywhere in the world;

- "**Accountability**": intended as a clear identification of competent authorities and commitment to rule-based trade;

- "**Inclusion**": testified by the calls for comments from any entity or individual "globally" and by an essential reliance on "allies", that are clearly listed in the regulations[2].

These principles are to be justified by an attempt to fix global standards. In this sense one can understand more easily the American *longa manus* in export controls' outreach.

US export control regulations can essentially impact **anyone dealing with US controlled goods or technology**. Jurisdiction is claimed to extend not only to individuals or corporations of US nationality, but also on **companies incorporated in other countries**, in which US individuals or corporations have only some minimum level of shareholdings.

US laws attribute "**nationality**" also to US origin goods and technologies and even to foreign items incorporating certain US technology or having a design directly based on US technical data. Thus, American jurisdiction will follow the items, wherever located, and apply on companies with no US ownership as well as individuals with foreign nationality.

Extraterritoriality has been used in attempt to deter "triangulation". In the American perspective, a country must be able to ensure that sensitive or strategically important

[1] P. Holtom, M. Bromley, P. D. Wezeman and S. T. Wezeman, SIPRI Trends in International Arms Transfers 2012, Stockholm International Peace Research Institute, March 2013, http://books.sipri.org/product_info?c_product_id=455

[2] This opinion seems to be confirmed by the recent remarks by U.S. Trade Representative Michael Froman on the United States, the European Union, and the Transatlantic Trade and Investment Partnership, 30 September 2013, .

equipment or technology will not be simply redirected from a seemingly "safe" recipient to a third country or entity which might be a proscribed destination.

There is no commonly recognised basis in international law to underpin this **"extended" notion of jurisdiction**. However, some commentators have suggested that this issue might be overcome by its voluntary acceptance by the foreign individual or entity. When applying for an export licence, foreign entities are put on notice of US jurisdictional claims. Filing a request for authorisation will also include explicit acceptance of very specific "**submission clauses**" which are *verbatim* and cannot be modified.

In addition, the **US courts see much of the cross-border conduct as "territorial" in nature**. "Acts" being conducted on US territory will include even sending emails to the US, placing phone calls into the US, sending purchase orders or wiring money into the US, and also acts "caused to be done" in the US[3].

[3] "*A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act described in subsection (a) shall, upon conviction, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both*". 50 U.S.C. §1705(c). "*Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal*".18 U.S.C. § 2(b)

3. The Legal Context

3.1 International Legal Instruments

Collective efforts to promote cooperation in trade control and non-proliferation are organized and coordinated through intergovernmental *fora,* essentially aimed at promoting a common approach, international standards and harmonised control lists.

The most important are:

- the **Australia Group**, for controlling chemical production equipment and the proliferation of biological technology that could be "weaponised";

- the **Nuclear Suppliers Group**, to restrict the export and limit the proliferation of nuclear-related technology[4];

- the **Wassenaar Arrangement**, aimed at promoting transparency and greater responsibility in transfers of conventional arms and dual use goods and technologies;

- the **Missile Technology Control Regime**, focused on stemming the proliferation of missile technology capable of delivering weapons of mass destruction (WMD).

These multilateral systems have the advantage of allowing consultation and information exchange and foster internationally coordinated strategies. Participating States are generally asked to further implement controls in their national legislations and share information on restricted destinations.

However, while the number of international exporters of sensitive technologies is growing, there is often lack of consensus over the identification of the actors that present a proliferation threat, and negotiations in many instances have led to vague, informal and ambiguous provisions[5].

Furthermore, these international regimes do not have any authority to impose any standard or guideline directly on exporters and do not include sanctions for non-compliant participating States.

Decisions are implemented in consideration of national risk assessments and their enforcement is determined on *ad hoc* basis when deciding on the issuance of a licence.

While the United States generally presents itself as a traditional leader of non-proliferation regimes, in practice important national specificities persist as international agreements are

[4] Members include: Argentina, Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Kazakhstan, Latvia, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russia, Slovak Republic, Slovenia, Spain, South Africa, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States.
[5] M. Beck, "Reforming the Multilateral Export Control Regimes", in *The Nonproliferation Review*, Summer 2000, p.96.

implemented in the national legal system only once they are tailored to foreign policy considerations and national risk assessments.

3.2 The National Legal Framework

In the United States, export controls were born as a wartime measure: in 1775, one year before the signing of the Declaration of independence, the Congress outlawed the export of goods to Great Britain.

A series of successive acts gave the President legal basis for controlling the export of military significant goods and technology and limit economic activities with "enemy" countries or nationals of those countries[6]. After the Second World War, a new "peacetime" layout was designed. This involved the idea of a multilateral effort, together with North Atlantic Treaty Organisation (NATO) allies, to contain USSR ambitions through specific licensing requirements for soviet bloc countries[7].

The **Coordinating Committee for Multilateral Export Controls (CoCom)** was therefore established in 1949, as an informal "non-treaty" multilateral organisation through which the US and its allies attempted to maintain a NATO edge in defence technology and limit the flow of military technology to the Warsaw Pact countries'.

CoCom rules put in place a very restrictive system of control: the export of items on its "embargo list" (International List I) was prohibited and only limited amounts of items in the "quantitive" list (International List II) were allowed. The decision-making was based on consensus: every member could, in practice, veto others' proposed exports of controlled items.

In this view, the US enacted the "Export Control Act" that same year, in view:

> *"(1) to reduce continuing shortages in critical materials, (2) to aid the President in implementing foreign policy, and (3) to control items deemed critical to U.S. national security"*[8].

In 1969, concomitantly with a period of relative relaxation in the US-USSR relations, the Export Control Act changed its "defensive" approach to respond to growing political pressure, as trade was becoming more and more essential to the economies of both the US and its allies. Congress therefore passed the **Export Administration Act**, with a policy shift aimed at mitigating risks in a context of positive promotion of exports.

Since then, American export control related laws and their implementing regulations have revolved around the dilemma of guaranteeing national security without being detrimental to

[6] Ch. 10, 6 Stat. 411 (1917), as amended, 50 U.S.C. App. Sec 1–44 (1964).
[7] I. F. Fergusson, "The Export Administration Act: Evolution, Provisions and Debate", Congress Research Service, 7-5700, 15 July 2009, p.2, available online http://www.fas.org/sgp/crs/secrecy/RL31832.pdf.
[8] Export Control Act of 1949, Ch. 11, 63 Stat. 7, as amended, 50 U.S.C. App. Sec 2021–32 (1964). See also U.S. Congress, Senate Report 31, 81st Congress, 1st Session, 23 (1949).

economic wealth. The growing importance of trade to the US resulted in an act comprehensively rewritten in 1979.

After the collapse of the USSR and while CoCom was being replaced by the **Wassenaar Arrangement** in 1997, US started to perceive external threats differently and the system could be finally streamlined and in a sense, "liberalised".

However, **Storm Thurmond National Defence Authorisation Act for Fiscal Year 1999** made legal requirements for exports stricter while moving back the jurisdiction over satellites from the Department of Commerce to the Department of State[9].

As a result of the "liberalization phase", American telecommunication satellites were easily exported for launch on Chinese launch vehicles, which services were nationally subsidised and cheaper than any US, Russian or European option. However, two launch failures shed light on significant satellite technology transfers as technical information needed to be communicated to adapt satellites to launchers and as a result of the Chinese management of technical issues. Heated congressional debate followed the scandal, and finally led to **tougher controls, especially on space-related items** that were moved under Department of State's International Traffic in Arms Regulations (ITAR).

US Constitution and laws, in consistency with the "foreign commerce clause", consider **exports as a privilege which is granted to the economic operators and not a right**[10]. The transfer of strategically sensitive articles and services is thus subject to control of the US President, who has authority to set foreign and national policy objectives for international defence cooperation and military export controls under the 1979 Arms Export Control Act (AECA).

The **Export Administration Act (EAA) of 1979** is the statutory authority for dual-use export controls. It originally "expired" in 1989.
Congress can temporarily delegate to the executive branch its constitutional authority to regulate foreign commerce. However, when the foreseen period has lapsed, if the Congress has not reached an agreement, the President has normally declared a national emergency and has maintained export control regulations under an executive order[11].

The EAA has thus been periodically re-authorised for limited periods of time, more recently until August 2001. The licensing system created under EAA is currently continued by a

[9] Congressional Record, V. 145, Pt. 14, August 4, 1999 to August 5, 1999.
[10] Q. Michel, S. Paile, M. Tsukanova, A. Viski, *Controlling the Trade of Dual-Use Goods, A Handbook,* Non-proliferation and security No 9, Peter Lang, Brussels, Bern, Berlin, Frankfurt Am Main, New York, Oxford, Wien, 2013, p.73.
[11] I. F. Fergusson, R.D: Shuey, C. Elwell, J. Grimmet, "Export Administration Act of 1979 Reauthorisation", CRS Report for Congress, 11 March 2002, http://www.fas.org/asmp/resources/govern/crs-RL30169.pdf

presidential declaration of national emergency and the invocation of **International Emergency Economic Powers Act (IEEPA)**, which confers upon the President the authority to:

> *"investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States"*
> *"by any person, or with respect to any property, subject to the jurisdiction of the United States"*[12].

3.3. Who controls?

The US export control environment consists of a myriad of regulations issued and administered by a set of multiple agencies of the US Federal government.

Departments of Commerce, Defence, State, Treasury, Energy and Interior, the Nuclear Regulatory Commission, all intervene in the governance of export controls under various statutory sources:

- Export and re-export of "dual use" items and technology is authorized by the **Bureau of Industry and Security of the Department of Commerce** under the Export Administration Regulations (EAR);

- Inherently military technologies are controlled by the **Department of State and its Department of Defence Trade Controls (DDTC)** based on International Traffic in Arms Regulations (ITAR)[13];

- The **Office of Foreign Assets Control (OFAC) of the Department of Treasury** administers the implementation of economic embargos and sanctions that affect not only exports and re-exports, but also imports and financial dealings;

- The **Department of Energy** is competent for the licensing of the nuclear technology[14];

- The **Nuclear Regulatory Commission**, controls the import and export of nuclear materials and equipment[15];

[12] US Code Title 50, Chapter 35, § 1702 (B), http://www.treasury.gov/resource-center/sanctions/Documents/ieepa.pdf
[13] DDTC is a component of the Bureau of Political and Military Affairs and consists of four offices: Management, Policy, Licensing and Compliance.
[14] It also licences the export of electric power to Mexico and Canada and the export of natural gas.

- The **Department of Defence**, although not a licensing agency, has important reviewing and advising functions[16].

The power to conduct investigations into export control violations is also diffused among several enforcement agencies:

- The Immigration and Customs Enforcement (ICE) of the **Department of Homeland Security (DHS)** and the **Federal Bureau of Investigation (FBI)** have investigatory authority involving the Arms Export Control Act (AECA), the Export Administrations Regulations (EAR), the International Emergency Economic Powers Acts (IEEPA), as well as sanctions violations overseas[17];

- The **Department of Commerce** administers cases involving EAR and IEEPA violations through the Office of Export Enforcement (OEE) at the BIS[18];

- The Office of Defence Trade Compliance (ODTC) at the Directorate of Defence Trade Controls (DDTC) of **Department of State** deals with internal civil enforcement actions (i.e. consent agreements, debarments, transaction exceptions, charging letters, policies of denial, etc.) and provides agency support to ICE and FBI;

- The Office of Enforcement of the **Nuclear Regulatory Commission (NRC)** investigates violations related to nuclear material and facilities, and refers violations to

- the **Department of Justice**, that undertakes criminal prosecutions resulting from investigations by licencing agencies, ICE and FBI;

- The **Department of Defence** controls the enforcement of export controls of sensitive defence technologies to proscribed destinations through its Defence Criminal Investigation Service (DCIS).

Such a multitude of actors implies a need to coordinate information sharing and a possibility of enforcement conflicts and interagency disputes.

---

[15]This divided competency on nuclear issues is due to historical reasons: NRC was formed in 1975 as an independent agency of the US government, to take over the role of US Atomic Energy Commission and take care of the oversight of nuclear energy matters, nuclear medicine and nuclear safety, while the development of nuclear weapons was transferred to the Energy Research and Development Administration (ERDA), that in 1977 became the US Department of Energy.See USNRC, History, http://www.nrc.gov/about-nrc/history.html#nrctoday

[16]Q. Michel, S. Paile, M. Tsukanova, A. Viski, *Controlling the Trade of Dual-Use Goods, A Handbook,* Non-proliferation and security No 9, Peter Lang, Bruxelles, Bern, Berlin, Frankfurt Am Main, New York, Oxford, Wien, 2013, p.73.

[17] ICE investigates violations of dual use and munitions export controls, transfers to sanctioned countries and embargoed destinations, supplements and supports BIS and DDTC, while FBI's WMD Directorate receives and analyses intelligence on proliferation networks and cooperates with export licencing agencies.

[18] OEE refers civil violations to the Office of Chief Counsel at BIS and criminal violations to DOJ.

Improvements have been made in 2010 as a result of President Obama's Executive Order 13558 establishing the **Export Enforcement Coordination Centre (E2C2),** among the Departments of State, the Treasury, Defence, Justice, Commerce, Energy, and Homeland Security as well as the Intelligence Community[19]. Active since 2012, this multi-agency centre is aimed at guaranteeing a more robust whole-of-government approach while facilitating intelligence and information sharing between eight US governmental departments and 15 federal agencies[20].

3.4 What is controlled?

3.4.1 The classification of items to be exported

A primary issue concerns "**what is controlled**", *i.e.* the determination of items subject to restrictions.

The classification of items plays a fundamental role in the US export control system. Determining if the items that need to be exported are subject to obligations under the export control regulations will allow to tell:

- whether they are subject to control,
- under which jurisdiction, and
- if the transfer must be authorized through issuance of an export authorisation or "licence" or otherwise qualifies for a "licence exception" (and can thus be exported without applying for an authorisation).

To establish whether a licence is required prior to the export the most important step will be the **classification of the item to be exported**: several lists and corresponding categories will need to be checked to identify the regulations that will be applicable (or "jurisdictional status").

After that, its "classification status" will need to be determined, by examining all the categories and identifying where the item is described. Only after these steps are followed, it will be possible to determine if an authorisation is required to export.

[19] The Department of Homeland Security administers the E2C2 and provides its Director. There are two Deputy Directors, one from the Department of Commerce and one from the Department of Justice.
[20] See "Export Enforcement Coordination Center (E2C2)", Export.gov http://export.gov/%5C%5C/e2c2/index.asp

The person exporting or re-exporting an item is responsible for determining the jurisdiction and classification status. Determining the correct jurisdiction and classification status is vital to avoid potential and successive violations[21].

3.4.2 A list-based approach

Multilateral export control regimes generally agree on common lists or at least on general guidelines that should orientate the drawing up of national lists of controlled items. However, each State will implement these principles based on national considerations, taking into account foreign policy objectives but also national technological excellences.

To this aim, several lists are issued and regularly updated by the Federal Agencies involved:

The **Commerce Control List (CCL)** catalogues the items controlled under the EAR. These Regulations generally refer to items controlled as "dual use", which denotes "*EAR-controlled items that can be used both in military and other strategic uses (e.g. nuclear) and commercial applications*".[22]Items under the jurisdiction of the Commerce Department generally cover goods and technology which are designed for commercial purposes but can have potential military applications, like in the case of aircraft, computers, mapping software, or pathogens. Each controlled item has an "Export Control Classification Number" (ECCN), an alpha-numeric code[23], based on the 10 categories listed in the Wassenaar Arrangement[24] and their functional groups (equipment, assemblies and components) and accompanied by a description of the item and licencing requirements (or "reasons for control").

The list is similar to the list of items that is annexed to European Regulation n.428/2009 on the control of exports, transfer, brokering and transit of dual use items within the European Union. Both lists reflect multilateral engagements under the Wassenaar Arrangement, however the EU list also includes requirements under Nuclear Suppliers Group, the Australia Group, and Missile Technology Control Regime[25].

---

[21] See also "Items Subject to the Jurisdiction of the International Traffic in Arms Regulations are Controlled as "Defense Articles at the Point of Manufacture", p.2, http://www.pmddtc.state.gov/documents/Jurisdictional_Policy_Document.pdf

[22] EAR specify that the precise description of what is "subject to the EAR is in n § 734.3, which does not limit the EAR to controlling only dual-use items. "The EAR control any item warranting control that is not exclusively controlled for export, re-export or transfer […] by any other agency of the US Government ot otherwise excluded from being subject to the EAR […] Thus, items subject to the EAR include purely civilian items, items with both civil and military, terrorism or potential WMD-related applications, and items that are exclusively used for military applications but that do not warrant control under the International Traffic in Arms Regulations (ITAR)", See § 730.3 EAR *"Dual use" and other types of items subject to the EAR*.

[23] E.g. 3A001.

[24] (1) Nuclear materials, facilities, and equipment; (2) materials, organisms, microorganisms, and toxins; (3) materials processing; (4) electronics; (5) computers; (6) telecommunications and information security; (7) lasers and sensors; (8) navigation and avionics; (9) marine and (10) propulsion systems, space vehicles, and related equipment

[25] Additional discrepancies between the lists might also derive from eventual time shifts in implementation of changes adopted under the several multilateral engagements.

- The Department of State's **US Munitions List (USML)** designates defence articles and services controlled under the International Traffic in Arms Regulations (ITAR)[26]. It also includes items considered as "Significant Military Equipment" (SME) (articles for which special export controls are warranted, indicated by an asterisk), and MTCR related items, which are listed in a specific Annex. USML's 21 Categories range from firearms, armaments and ammunitions to guided missiles, spacecraft and nuclear weapons to electronics, military training and auxiliary military equipment.

- Controlled nuclear items are listed in the **Nuclear Regulatory Commission Controls (NRCC)**, including nuclear equipment and materials, such as those in Part I of the NSG Guidelines.

Articles that are on none of the lists may be classified as EAR99, a general "basket" category that covers items "subject to EAR"[27] but not listed on CCL.

The majority of products that are normally commercialised is designated as EAR99 and in general does not require a licence to be exported or re-exported, but can be shipped under the designation of **"NLR" which stands for "No licence required"**.

Generally EAR99 articles are widely traded, low technology consumer goods. However, they may require a licence if exported to an embargoed country, end-user of concern or destined to a prohibited end-use[28]. It is therefore important to obtain information from the American exporter on the classification of the item, and to check the "watch lists" of destinations of concern.

Definitions are generally very sophisticated, and require a minimal technical knowledge of the product. **The list on which the item is included will determine the compliance obligations**. "Intended use" after the export is not relevant in determining jurisdiction: if an item is listed on the US Military List it will be subject to ITAR regulations, even if the exporter might claim a *de facto* civilian use.

Some items might be listed on both lists. It is especially the case for some of the items listed on the Missile Technology Control Regime (MTCR) Annex, controlled by both the Department of Commerce on the CCL and the Department of State on the USML[29].

If doubt exists concerning the jurisdiction of an article or service, the Department of State allows the filing of requests for "**Commodity Jurisdiction**" (CJ), upon electronic submission of a CJ determination form[30]. The form requires very detailed information on the item, history of its design, development and use, and foreign availability.

---

[26]Designation of articles and services deemed to be defence articles and defence services is made by the Department of State with the concurrence of the Department of Defence.
[27] See § 7342 (a) EAR "*Subject to the EAR- Definition"*
[28] See Paragraph 3.4.2 A list-based approach
[29] 22 CFR 121.16 - Missile Technology Control Regime Annex.
[30] DS-4076. See Commidity Jurisdiction FAQs, http://www.pmddtc.state.gov/faqs/documents/FAQ_CJ.pdf.

3.4.3 The categories of items that are subject to control

Items and services subject to control include a wide variety of categories.
Together with "tangible" commodities, objects which can be "grasped" and to be exported require a "physical" crossing of the border, like goods**,** equipment, parts, materials and components, controls apply also to **"intangible"** transfers like technical data or the provision of technical assistance.

Under the EAR, Part 772 defines:

- "**equipment**" as a "*combination of parts, components, accessories, attachments, firmware, or software that operate together to perform a function*",

- "**components**" or "assemblies" as items that are useful only when used in conjunction with an "end item", and

- "**material**" as "*any list-specified crude or processed matter*".

"Software" is defined under EAR as "*a collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression".*

"Technology" will be also subject to control. Its definition follows the one internationally agreed by the international non-proliferation *fora* : "*specific information necessary for the "development", "production", or "use" of a product".* It covers both "**technical assistance**" (instruction, skills training, working knowledge consulting services) and "**technical data**" (blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions)[31].

ITAR regulations define, more generally:

- a "**defence article**" as any item or technical data designated in the USML, and specify that "*this term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designed in* [the USML]. *It does not include basic marketing information on function or purpose or general system descriptions",* and a

- "**defence service**" as : "*(1) the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarisation, destruction, processing or use of defence articles; (2) The furnishing to foreign persons of any technical data controlled [..] whether in the United States or abroad; or (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical,*

[31] See also Q. Michel, S. Paile, M. Tsukanova, A. Viski, *Controlling the Trade of Dual-Use Goods, cit.*, p.82.

educational or information publications and media of all kinds, training aid, orientation, training exercise, and military advice".

Items controlled cover not only articles or services produced or originated in the United States, but **also foreign made products** that contain more than a certain percentage of US controlled content (*de minimis*), foreign made products produced based on US technology or software or made by a plant or major component of a plant located outside the US, which is direct product of certain US technology or software[32].

3.4.4 The Controlled Movements

The US export control legislation and implementing regulations cover a **wide definition of what qualifies as an "export"**, including a variety of transhipment, import, brokering, transfer and re-export of controlled items.

EAR generally defines an "export" as any "*actual shipment or transmission of items out of the United States*"[33] but points out that "***some provisions give broad meaning to the term "export", apply to transactions outside the United States, or apply to activities other than exports***"[34].

The exporter is warned that the scope of exports shall include "*certain actions that you might not regard as an export in other contexts*", including **any oral, written, electronic or visual disclosure, shipment, transfer or transmission of commodities, technology, information, technical data, assistance or software codes to**:

- Any person or entity outside the US including US citizens
- Any non-US individual wherever they are ("deemed export")
- A foreign embassy or affiliate.

ITAR definition of export recalls the same basic principles but is more detailed as includes:

- "*sending or taking a defence article out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data"*

- "*transferring registration, control or ownership to a foreign person of any aircraft, vessel or satellite covered by the US Munitions List, whether in the United States or abroad"*

[32] US Department of Commerce, Bureau of Industry and Security, Office of Exporter Services, *Guidance on the Commerce Department's Reexport Controls, https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CFEQFjAD&url=http%3A%2F%2Fwww.bis.doc.gov%2Findex.php%2Fforms-documents%2Fdoc_download%2F4-guidelines-to-reexport-publications&ei=4rtmUqbZB67X7AauYHwCg&usg=AFQjCNHI88sAWuYPaVpyHQsN8DMCand_4g&sig2=Wg5Zd1UW0_wS257QDkoIcA*

[33] See §734.2(b) EAR, "*Export and re-export"*

[34] See §730.5 EAR, "*Coverage of more than exports*".

- "*disclosing (including oral or visual disclosure) or transferring in the United States any defence article to an embassy, any agency or subdivision of a foreign government (e.g. diplomatic missions)*" or

- "*disclosing or transferring technical data to a foreign person, in the US or abroad"*

- "*performing a defence service on behalf of, or for the benefit of, a foreign person, whether in the US or abroad*"[35].

3.4.4.1 "Deemed Export"

The notion of "**deemed export**" is very specific to American regulations.

Under §734.2(b)(2)(ii) EAR, it is said to occur **whenever there is release of controlled technology (or source code) to a foreign national.** "Release" of controlled technology can take place through training, oral exchange, practical demonstration or even visual inspection and is "deemed to be an export" to the home country or countries of the foreign national[36].

Furthermore, law cases have determined that the possibility to access controlled data is sufficient to originate a violation[37]. In other terms, it is not necessary to prove that there is actual transfer of information, **the simple possibility to have accessed the information is sufficient**. In 2004 General Dynamics and General Motors agreed to pay 20 million $ because investigations had shown that after the acquisition of General Dynamics by GM, Dual Nationals had computer access to databases and servers containing ITAR-controlled defence articles and technical data.[38]

This issue is particularly critical to **Universities, high technology research and development institutions and ICT sectors**. Sanctions to Universities are not uncommon. In 2008, University of Tennessee professor Dr. J. Reece Roth was convicted of unlawfully exporting information on US Air Force sponsored research to foreign nationals, in particular a Chinese research assistant in his laboratory, without appropriate export authorisation. Dr Roth was sentenced to 48 months prison for the violation.[39]

The State Department, in its "Guidelines for Implementing New Dual National/Third Country National Policy for Agreements", reminds that, when requested to issue a licence for the export of defence articles and services, and notably technical data or information, the

[35] See §120.17 ITAR, "*Export"*.
[36] ITAR does not use the term "deemed export" as it is used under the EAR, but the notion is the same under both EAR and ITAR.
[37] See Department of State, Directorate for Defence Trade Controls, Draft Charging Letter, Investigation of General Motors Corporation, http://pmddtc.state.gov/compliance/consent_agreements/pdf/GeneralMotorsCorp_DraftChargingLetter.pdf
[38] See Department of State, Directorate for Defence Trade Controls, Draft Charging Letter, Investigation of General Motors Corporation, http://pmddtc.state.gov/compliance/consent_agreements/pdf/GeneralMotorsCorp_DraftChargingLetter.pdf
[39] See Department of Justice, "Retired University of Tennessee Professor Convicted of Arms Export Violations", 3 September 2008, http://www.justice.gov/opa/pr/2008/September/08-nsd-774.html

Department for Defence Trade Controls (DDTC) "*does consider the* ***country of origin or birth in addition to citizenship***"[40].

A licence might be needed also if the product is US originated but export is being made from a third country to a fourth country. US export controls also cover "**re-exports**", defined in part 772 EAR as any "*actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country"* and in part 120.19 ITAR as "*the transfer of defence articles or defence services to an end-use, end-user or destination not previously authorized by licence, written approval or exemption pursuant to this subchapter".*

EAR specifies that transit or transhipment constitute "deemed exports", while for purpose of satellites controlled by the Commerce Department, **re-export will also include the transfer of registration of a satellite** or operational control over a satellite from a party resident in one country to a party resident in another country.

3.4.4.2 Brokering activities

Since 1996, **brokering activities** are controlled under the ITAR, with respect to manufacture, export, import or transfer of any defence article listed on the USML.

A "broker" has been generally defined as "*anyone who acts as an agent for others in negotiating or arranging contracts, purchases, sales or transfers of defence articles or services in return for a fee, commission or other consideration"*[41]. Since October 2013, its definition has been widened to include any person "*who engages in brokering activities"* including **any action on behalf of another to facilitate the manufacture, export, permanent import, transfer, re-export or retransfer of a US or foreign defence article or defence service**.

For each transaction, including the financing, transportation, freight forwarding or any other action that is aimed at facilitating manufacture, export, import or transfer of a defence article or service, it will be necessary to register with the Department of State and obtain the necessary authorisation. And this shall be applicable for "any defence article or service, irrespective of its origin".

Registration as a broker entails also an obligation to submit an annual report to the US government enumerating and describing activities and exemptions used.

The rule does not apply to foreign persons outside the United States who are not owned or controlled by a US person.

[40] US Department of State, Directorate of Defence Trade Controls, *Guidelines for Implementing New Dual National/ Third-Country National Policy for Agreements*", 25 July 2011, http://www.pmddtc.state.gov/licensing/documents/D-TCN_AG_GuidanceFinal.pdf

[41] See Part 129.2 ITAR.

3.4.5 The controlled destinations and licencing policies

Exports are restricted by item, but also based on the **country of destination** and the **recipient entity**.

The **EAR include a "Country Chart"**[42] where licensing requirements for dual-use items result from the combination of reasons for control and final destination. Exports of strategic and defence-related items to certain countries are restricted based on adherence to UN arms embargoes or unilateral risk assessments.

1979 Export Control Act essentially restricts the **exports that could improve the military capabilities of "enemy country"** resulting in a threat to US national security.

For **defence articles or services**, the Arms Export Control Act (AECA), in its Section 3(a), clearly specifies the general criteria for countries and international organisations to be eligible to receive them. Section 4 imposes to sell such items only to "**friendly countries**" and exclusively:

- for use in internal security;
- for legitimate self-defence;
- to enable the recipient to participate in regional or collective arrangements or measures consistent with the UN Charter;
- to enable the recipient to participate in collective measures requested by the UN;
- to enable the foreign military forces in less developed countries to construct public works;
- to engage in other activities helpful to the economic and social development of such friendly countries.

It must be noted that **Canada benefits of a limited exemption**, as it is considered part of the "US defence industrial base"[43].

Special comprehensive export authorisations exist for **NATO, Australia, Japan and Sweden** for "major projects", "major programs" or "global projects" under specific requirements[44]. In addition, under bilateral treaties[45] with the **United Kingdom and**

[42] Supplement No. 1 to part 738 of the EAR
[43] For ITAR, see Part 126.5, "Canadian exemptions".
[44] See Part 126.14 ITAR, "Special comprehensive export authorisations for NATO, Australia, Japan and Sweden".
[45] See Defence Trade Cooperation Treaty between the United States and the United Kingdom.

Australia, certain defence articles are exempt from licencing obligations to approved end-users in those countries[46].

Certain transactions with countries subjects to **boycotts, trade sanctions and embargoes** are under jurisdiction of the Department of Treasury (DoT). Transactions might be subject to country-specific sanctions and therefore require a licence issued by the Office of Foreign Assets Control (OFAC). These controls generally concern US persons but certain programs, such as those regarding Cuba, Iran or North Korea, also require foreign persons in possession of US origin goods to comply[47].

The "list-based approach" followed in the determination of which items are subject to control also extends to identification of sensitive destinations and determination of licence requirements.

3.4.6 EAR licensing policy

As underlined before[48], The Commerce Control List contains ECCNs with a description of the category of items controlled, accompanied by "**reasons for control**".

The licensing policy for dual use commodities includes controls for:

AT	Anti-terrorism
CB	Chemical and Biological Weapons
CC	Crime Control
EI	Encryption Systems
FC	Firearms Convention
MT	Missile Technology
NS	National Security
NP	Nuclear Non-proliferation
RS	Regional Stability
SS	Short Supply
SI	Significant Items
SL	Surreptitious Listening
UN	United Nations Sanctions

Restrictions vary from country to country. EAR essentially separates foreign countries into five country groups (from A to E), distinguishing between:

- "**Controlled countries**" defined by Part 772 as countries controlled for national security purposes under the authority of DoC and listed in "Country Group D:1"[49].

[46] See Parts 126.15 "Expedited processing of license applications for the export of defence articles and defence services to Australia or the United Kingdom" and 126.17, "Exemption pursuant to the Defence Trade Cooperation Treaty between the United States and the United Kingdom".
[47] Office of Foreign Assets Control, OFAC FAQs "Who must comply with OFAC regulations?", ,http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx#1
[48] See 3.4.2, A list-based approach

- "**Cooperating countries**" that cooperated with former CoCom member countries in restricting strategic exports[50]

- "**Countries supporting international terrorism**": In accordance with §6(j) of the Export Administration Act of 1979, as amended, the listed governments are considered to have repeatedly provided support for acts of international terrorism[51].

Key elements are the "**end use**" and **ultimate destination**. For instance, pursuant to the embargo on Cuba, nearly every item that is subject to the EAR will require an appropriate licence for export[52].

In order to determine the applicable licence requirements, the exporter will have to match:

- the reasons for control listed in the ECCN entry on the CCL and
- the country of destination in the Country Chart.

Even if an export license would normally be required for the destination of export, a "**Licence Exception**" may be available. Exceptions are authorisations that, under stated conditions, allow export, re-export or transfer (in-country) without a licence[53]. Listed in Part 740 EAR, exceptions bear a three letters symbol:

LVS	Shipments of limited value
GBS	Shipments to Country Group B
CIV	Civil end-users
TSR	Technology and software under restriction
APP	Computers
TMP	Temporary imports, exports and re-exports
RPL	Servicing and replacement of parts and equipment
GOV	Governments, international organisations, international inspections under the Chemical Weapons Convention, and the International Space Station
GFT	Gift parcels and humanitarian donations
TSU	Technology and software- unrestricted
BAG	Baggage
AVS	Aircraft and vessels
APR	Additional permissive re-exports
ENC	Encryption commodities, software and technology

[49]Including: Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, the People's Republic of China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Macau, Moldova, Mongolia, North Korea, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam. All of the controlled countries except Cuba are listed in Country Group D:1 of the EAR. Cuba is listed in Country Group E:2.

[50] Austria, Finland, Hong Kong, Ireland, Korea (Republic of), New Zealand, Sweden and Switzerland

[51]Cuba, Iran, North Korea, Sudan, and Syria.

[52] 15 C.F.R. §746.2.

[53] § 730.7 "Licence requirements and exceptions".

AGR	Agricultural commodities
CCD	Consumer Communications Devices
STA	Licence Exception Strategic Trade Authorisation

The use of exceptions is subject to restrictions, listed in Part 740.2.

Part 742 describes the licencing policies that BIS will apply in reviewing the application. BIS generally adds **conditions** to nearly all export licences. Conditions are the result of an interagency process that involves BIS, the State and Defence Departments and may restrict the possible use of an item after the export or require certain reports to be made by the exporter[54].

Parts 748 and 750 EAR provide information on license submission and processing. Under BIS application guidelines, in case of transfer of **controlled technical data requirements** exporters will have to include detailed information concerning the foreign transferee that will receive data, but also its foreign employees, including names, passport number and addresses. In addition, a resumé for each individual, showing education, employment history and military service must be provided for each of them. The US exporter will have to obtain amendments each time the foreign company hires new employees in the affected program area[55].

The Department of Commerce must review the application and refer it to the eventual reviewing agencies within 9 days of receipt. The latters have 30 days to respond with recommendations: as a result, the licence application will be either approved, approved with conditions or denied.[56]

In case of denial, part 756 EAR provides rules for filing appeals.

3.4.7 ITAR licencing policy

The licensing policy under ITAR requires a **licence for exports of almost all items on the USML**.

Unlike some dual use controls, licensing requirements are based in principle on the nature of the article and not the end-use or end-user of the item.

Prior licence will also be required **before**:

- **Reselling, transferring, re-exporting, retransferring, transhipping, or disposing of any defence article** to any end-user, end use or destination other than stated on the export licence

[54] Bureau of Industry and Security, US Department of Commerce, *Don't Let This Happen To You, An Introduction to US Export Control Law",* September 2010,p.23 https://www.bis.doc.gov/index.php/forms-documents/doc_view/535-don-t-let-this-happen-to-you-2010
[55] C. Bums, "Naming Names", Export Law Blog, 7 November 2013, http://www.exportlawblog.com/archives/5539#!
[56] In CY 2012, BIS average processing time for licence applications was 26 days.

- **Establishing a warehouse or distribution point** abroad for defence articles exported from the US (Warehouse Distribution Agreement)

- **Any performance of a defence service or disclosure of technical data** ("Technical Assistance Agreement")[57].

A licence will be required:

- for permanent exports of unclassified defence articles and related technical data
- for temporary import or export of unclassified defence articles[58]
- for permanent or temporary export or import of classified defence articles and related technical data
- for export of defence articles and services sold under the Foreign Military Sales Program.

While a specific focus on the sensitive nature of controlled items means that a DDTC licence will be required in almost all cases when the item to be exported is listed on the USML, ITAR licencing policy also takes into account the country of ultimate destination[59]. Any export of these very sensitive items has **presumption of denial for proscribed destinations**[60].

Although a specific "Country List" is not included in ITAR, it is clearly stated that a policy of denial applies to:

- Belarus, Cuba, Eritrea, Iran, North Korea, Syria and Venezuela

- The countries for which the US maintain an arms embargo (Burma, China, the Republic of the Sudan, etc.)[61]

- All export which "*would not be in furtherance of world peace and the security and foreign policy of the US*".

The same policy applies to:

- Shipments on vectors owned or operated by, or leased to or from, any of the proscribed areas

- Exports and sales prohibited by UN Security Council embargoes

- Exports to countries which the Secretary of State identified as supporting acts of international terrorism

[57] § 120.22 ITAR.
[58] "Temporary exports" are, under Part 123.5 ITAR, exports meant to last for a period of less than 4 years and then to be returned to the United States.
[59] A series of exceptions are listed in Part 123.16 ITAR.
[60] See Part 123.9, "Country of Ultimate Destination and Approval for re-exports or retransfers".
[61] Arms embargoes are published in State Department notices in the Federal Register.

- Sales, re-exports, retransfers and proposals to sell, export, transfer, re-export or retransfer ITAR controlled items to the abovementioned countries, including embassies or consulates.

- Exports to Iraq, Afghanistan, Democratic Republic of Congo, Haiti, Vietnam, Somalia, Sri Lanka, Liberia, Fiji, Cote d'Ivoire, Cyprus, Zimbabwe, Lebanon and Republic of Sudan, with some exclusions.

The notion of "**country of ultimate end use**" is fundamental to obtain an export authorisation, the objective being to avoid that very sensitive items de facto are exported for military uses or end up in "unsafe" hands. In determining the end-user and end-use, the exporter is expected to apply "due diligence" and review all readily available information, including information generally available to the public or available from other parties to the transaction.

"**Non-transfer and use assurances certificates**" are required for the export of items identified as SME (Significant Military Equipment) but also for some other defence articles, to guarantee that the foreign consignee and end user will not re-export, resell or otherwise dispose of the item outside the country named as location of the end use[62].

In case of **transfer of controlled technical data**, requirements under DDTC application procedures are less burdensome than BIS, as the important element concerns nationality of third country and dual nationals. The US exporter will thus need to list only the nationality of the employees concerned and amendments will be necessary only if new employees are hired in the affected program and their nationality is not previously approved[63].

Vessels, aircrafts and satellites covered by the USML are subject to special provisions: transferring registration or control to a foreign person is, when such items are concerned, considered as an export and will thus require licence or written approval from DDTC whether the aircraft, vessel or satellite is physically located in the US or abroad[64]. The same provision applies for registration in a foreign country of any of the abovementioned items when they are located in the United States.

As a result of the National Security Presidential Directive (NSPD-56) of 2008, the review and adjudication of licences under ITAR are to be completed within 60 days, except when certain national security exemptions apply[65].

3.4.8 The watch lists

A licence application may be necessary even if an export authorisation is not required for the country of destination or a licence exception would, in principle, apply.

---

[62] See Part 123.10 "Non Transfer and Use assurances"
[63] C. Bums, "Naming Names", Export Law Blog, 7 November 2013, http://www.exportlawblog.com/archives/5539#!
[64] See Part 123.8, "Special Controls on Vessels, Aircraft and Satellite covered by the US Munitions List".
[65] I. F. Fergusson, Paul K. Kerr, "The US Export Control System and the President's Reform Initiative", Congressional Research Service, 7-5700, 20 September 2013, p. 6, http://www.fas.org/sgp/crs/natsec/R41916.pdf

Special restrictions and licence requirements apply to specific individuals and organisations: the export, re-export or transfer (within the same country) of all items subject to EAR, including EAR99, may be denied if the good is destined to a military end-use or to a "blacklisted" entity.

In this sense it is necessary to take into consideration the "**end user**". Part 772 EAR defines an "end-user" as "***the person abroad that receives and ultimately uses the exported and re-exported items***. *The end-user is not a forwarding agent or intermediary but may be the purchaser or ultimate consignee*".

There are several lists that may be relevant, and that include entities with which an exporter should refrain from doing business.

In case of enforcement investigations leading to unfavourable results, the BIS generally lists the entities that were subject to checks in the **Unverified List** that includes name, country and address of foreign persons who were party to a checked transaction whenever BIS was unable to conduct a pre-licence check or a post-shipment verification for reasons outside the US government's control or which existence or authenticity BIS was unable to verify[66].

When there is reasonable cause to believe that a foreign entity has been involved, is involved or poses a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the US, it is listed in the Commerce Department's **"Entity list"**[67], that catalogues names of businesses, research institutions, public and private organisations, but also individuals, together with the indication of their address, country, specific licence requirements and licence review policy that apply.

Other lists to be checked include:

- the **Denied Persons List (DPL)**, with the names of persons that have been denied export and re-export privileges by the **Department of Commerce** under EAR[68], and

- **Specially Designated Nationals and Blocked Persons List (SDN)**, published by the **Department of Treasury**'s OFAC. SDNs are individuals and entities "blocked" pursuant to the various sanction programs, terrorists or narcotics traffickers or entities that have otherwise been determined to be owned and controlled by, or act for or on behalf of other sanctioned groups or governments

- The **Debarred Parties List** is maintained by the **State Department** and lists the names of individuals who are barred by Part 127.7 ITAR from participating directly

[66] K.J. Kurland, "Export Control Reform: Compliance and Enforcement during Transition", presented at "Commerce and State Compliance and Enforcement", 18 July 2012, http://mtitv.com/Conference2012/PDF/commerce_and_state_and_enforcement_combined_update%202012.pdf

[67] The "Entity List" is found in Supplement No 4 to Part 744 EAR.

[68] US exporters and third parties in general are prohibited from dealing with denied parties in transactions involving US items.

or indirectly in the export of defence articles, technical data or defence services for which a licence or approval by the State Department is required.

The exporter should indicate in the licence application if a person listed is involved. In this case it is considered that the transaction carries a "**red flag**", an issue that should be resolved before the transaction, and that there is a high possibility of denial[69].

In general, exporters are exhorted to check these lists regularly, as additions and changes are very frequent. A "**Consolidated Screening list**", i.e. a downloadable file that consolidates export screening lists of the Commerce, State and Treasury Department is available on the website of "Export.gov". [70]

In addition, **"due diligence" is recommended in any transaction**. Before each transaction it is important to obtain information about the customer, the nature of its business, ownership and control and research the end use of the product.
Particular attention should be paid to:

- Private end users
- Lack of available information on the customer
- Proof of unfamiliarity with the articles to be exported and their use
- Statements or other documents that are not clear and legible
- Any reluctance to provide documentation.

[69] See http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
[70] http://export.gov/ecr/eg_main_023148.asp

3.4.9 "Contamination" of foreign produced products

US export control laws essentially attribute "nationality" to US-origin goods and technologies and claim jurisdiction on them wherever they are located and regardless the number of hands (and borders) they pass through.

But what happens **once components and technology are embedded in foreign items**?

American export controls will also cover articles produced elsewhere than in the US, whenever they are incorporating certain controlled US technology or have a design that is directly based on US technical data. This is generally known as the "contamination" principle.

Items controlled will therefore include not only commodities or services manufactured or originated in the United States, but also:

- **Foreign-made products** that embed more than a certain percentage of content controlled in the US under EAR (*de minimis*) or any percentage of US-origin defence articles or technology;

- **Derivative technology**, *i.e.* foreign made products produced based on US technology or software or made by a plant or major component of a plant located outside the US, which is direct product of certain US technology or software[71].

If foreign originated products embed more than a certain percentage value (***de minimis***) of US origin content controlled under EAR, the product will be subject to US export controls. If the product incorporates ITAR controlled components or technology, it is not relevant how important the component is in the overall value: even the smallest component will "contaminate" the product and make it ITAR-controlled (**"see through" rule**).

In case of derivative technology, direct products of US origin technology and the products of a plant or a major component of a plant developed based on US technology, will be subject to the EAR only if they are intended for specific controlled destinations and they would be subject to "national security" controls under the jurisdiction of the Commerce Department.

A foreign company that incorporates US origin parts or components in its commodities is responsible for its compliant use and export. It will therefore need to investigate if the product it has manufactured is subject to US export controls and "**contamination**" has taken place.

Since controls also extend to technology, it has to be kept in mind that "contamination" can occur through sending technical data to another country or another non-US person via any tangible or intangible mean like telephone calls, fax or email, access via servers or websites.

[71] US Department of Commerce, Bureau of Industry and Security, Office of Exporter Services, "Guidance on the Commerce Department's Reexport Controls".

It can also occur through "deemed export", for instance when a person with dual nationality or nationality of a third country is employed and can access manufacturing facilities, technical documents, engineering databases or participate into discussions and meetings with other employees that would expose him to ITAR controlled documents, items or information[72].

It is therefore imperative for any exporter to **be prepared, include export control reasoning** in its process and **avoid contamination**:

- Establish a written export control policy, that includes "deemed exports"
- Require information from any customers, vendors and partners of any ITAR-controlled item or technology involved in a business
- Mark and limit physically and virtually access to ITAR-controlled technical data
- Maintain segregation areas for ITAR-controlled items
- Always notify of US content and applicability of US regulations
- Document all steps taken
- Secure proper authorisation
- Establish procedures for any risk of non-compliance
- Train employees

In order to avoid deemed exports, it will be necessary to adopt specific measures and appropriate procedures, eventually verify the need to request licences (for instance when there is a facility visit by a person with dual nationality or nationality of a third country, or in case of other relevant interexchange).

[72] On the notion of "deemed exports", see 3.4.4 The Controlled Movements, *supra.*

3.5 Enforcement and sanctions

Various enforcement mechanisms exist to **ensure compliance with export control laws while preventing and deterring violations**.

In the United States, export control enforcement is based on the 1979 Export Administration Act (EAA), as amended[73]. Five agencies are primarily responsible: the Departments of Commerce, Homeland Security, Treasury, State and Justice.

US Customs officials (part of the Department of Homeland Security) have the authority to check any import or export and its licence at the borders. However, it is **Commerce Department's BIS** that **has primary responsibility** in export enforcement, as its jurisdiction covers the widest range of items and technology. By implementing the EAA, the EAR[74] place legal responsibility on persons who have information, authority or functions relevant to carrying out transactions subject to the regulations, including exporters (American or foreign), freight forwarders, carriers, consignees and other participants in an export transaction[75].

BIS conducts **selective end-use checks** on exports in "dual use" goods, to monitor compliance with requirements, verify the existence of non-licenced transactions, but also to confirm the end use and the company's reliability. Checks are carried out for **pre-licence, post-licence, or post-shipment inquiries.**

In case of violations, severe **civil and criminal penalties** may be assessed against both individuals and organisations.

Under the International Emergency Economic Powers Enhancement Act (IEEPA), for administrative cases pending or commenced on or after October 16, 2007 violations of the EAR can entail:

- Civil penalties per violation amounting to the greater of 250000$, or twice the amount of the transaction that determined the violation

- Criminal fines for wilful violations may be fined up to 1 M$ and/or up to 20 years of imprisonment.

In addition, under Section 11(h) of the 1979 EAA, administrative penalties may include **denial of export privileges for up to ten years** from the date of conviction. In this event, the convicted person would be prohibited from participating in any way in any transaction subject to the EAR. Any person that is determined to participate in any transaction under the EAR that involves a denied person will thus commit a violation. Furthermore, "**Temporary**

[73] 50 U.S.C. app. §§ 2401- 2420 (2000))
[74] As noted before, the EAR are continued under IEEPA's authority in times when the EAA is expired.
[75] 15 C.F.R. Parts 730-774 (2010)

Denial Orders", issued for 180 days and renewable, may allow denial of export privileges to prevent an imminent or on-going export control violation[76].

The names of denied persons are published in the Federal Register, which is also available online on Government Printing Office Access Website. The updated list of persons which have been denied export privileges is also accessible on the BIS website.

The **Office of Foreign Assets Controls (OFAC) administers and enforces several trade and economic sanction programs** against foreign countries and individuals. In addition, the Trading with the Enemy Act gives authority to the President to restrict foreign trade during wartime[77], and IEEPA allows the same restrictions on the basis of "any unusual and extraordinary threat" that determines a national emergency[78].

Penalties and criminal sanctions for violations of OFAC regulations under the IEEPA and under the Trading With the Enemy Act can be severe.

Depending on the program:

- Civil penalties for violations of the Trading With the Enemy Act can range up to $65,000 for each violation

- Civil penalties for violations of the International Emergency Economic Powers Act can range up to $250,000 or twice the amount of the transaction

- Civil penalties for violations of the Foreign Narcotics Kingpin Designation Act can range up to $1,075,000 for each violation

- Criminal penalties for wilful violations can include fines ranging up to $20 million and imprisonment of up to 30 years.

While penalties can vary widely, most of them are the result of settlements with foreign banks that evaded OFAC sanctions in order to allow transfers to sanctioned entities or destinations.

The State Department guarantees enforcement through the "Blue lantern" program[79], that monitors end-users, consignees and end use of defence articles and services and brokering activities to verify the *bona fides* of foreign consignees and end users and ensure respect of the compliance requirements through pre-licence, post-licence, or post-shipment verification. The program is performed worldwide by US Embassy personnel in cooperation with host governments. Every year its results are published on internet in reports that detail the number of checks initiated in the fiscal year of reference, countries targeted, and outcomes, with the objective to raise awareness about enforcement issues and warn

[76] See Supplement No 1 to Part 764of the EAR. For lists of controlled entities, *see 3.4.5 The controlled destinations and licencing policies.*
[77] 50 U.S.C. app. §5(b)(1)
[78] 50 U.S.C. §1701.
[79] As required by Section 40A of the Arms Export Control Act (AECA)

exporters about the need to pay attention to suspicious elements in transactions, or "red flags".

In case of export control violations administered by State Department's DDTC, AECA authorises the following sanctions:

- Civil penalties per violation up to 500000 $ per violation
- A maximum criminal penalty per wilful violations of up to 1 M $ and/or 20 years of imprisonment.

Most DDTC investigations are resolved through private remediation agreements and only a few result in public administrative orders. However, penalties and sanctions are always very important.
Similarly to BIS sanctions, DDTC can decide denial of export privileges under the ITAR, *i.e.* debarment from participating directly or indirectly in the export of ITAR controlled defence articles, technical data or defence services.

It is to be noted that **violations of one export control regime are not isolated from other regimes**. In 2011, Universal Inc. was convicted of violating the AECA for knowingly and wilfully attempting to export ITAR-classified military aircraft parts to Singapore without having obtained the necessary export authorisations from the Department of State. Negotiations of the administrative sanctions led to one year of probation, 1000 $ fine and a special assessment of 400 $. Although the violation essentially concerned State Department regulations, BIS also suspended export privileges for three years and revoked all licences issued under the EAR[80].

Business can be held liable for violations committed by companies that they acquire. Therefore export compliance policies of the target company (including export authorisations, the status of foreign employees who have access to control technologies and the existence of well-defined export procedures) will need to be taken into account to perform "due diligence" and avoid "successor liability". [81]

Sanctions can affect companies, but also individuals. CEOs can also be personally sanctioned with fines or imprisonment. On January 2013, Ji Li Huang, a Chinese national CEO of Ningbo Oriental Crafts Ltd. and his employee Xiao Guang Qi were sentenced 18 months and 250000$ fine, and 20000 $ fine respectively, for having conspired to steal trade secrets from Pittsburgh Corning Corporation, a company that produces FOAMGLAS® insulation. That same month, Timothy Gormley, the former export control manager of AR Worldwide/Amplifier Research in Souderton, PA, was sentenced 42 months in prison, 3 years supervised release and a 1000 $ fine in connection with the illegal export of microwave amplifiers to China and India.

[80] United States Department of Commerce, Department of Industry and Security, "Order Denying Export Privileges, in the Matter of Universal Industries Limited Inc., http://www.lexology.com/library/detail.aspx?g=fbea2a9b-f343-425d-baea-24a5c90bacdb

[81] Bureau of Industry and Security, US Department of Commerce, *Don't Let This Happen To You, An Introduction to US Export Control Law", cit.*, p. 55.

Freight forwarding companies are not immune from export control compliance obligations and sanctions: on May 2012, Ulrich Davis, former manager of a Netherlands-based freight-forwarding company, was condemned to 6 months prison for facilitating the illegal export of goods to Iran[82].

Recently, there has been a trend towards extending the scope of regulations to companies dealing with **insurances, automotive industries, financial institutions, ITC** but also exporters of less strategic goods when destined to specific destinations. On 26 November 2013, the Bureau of Industry and Security (BIS) announced that Weatherford International Ltd. in Houston, Texas, and four of its subsidiaries (collectively, "Weatherford") have agreed to pay a $50 million civil penalty following allegations that Weatherford exported oil and gas equipment to Iran, Syria and Cuba in violation of the Export Administration Regulations (EAR) and the Iranian Transactions and Sanctions Regulations (ITSR)[83].

3.5.1 Aggravating and mitigating factors

When determining the appropriate administrative penalty, **several factors are taken into account**.

BIS explicitly mentions the following:

- Destination of the export
- Degree of wilfulness involved
- Number of violations
- Criminal charges

Mitigating factors include:

- Voluntary self-disclosure
- Existence of effective export compliance programs[84]
- Cooperation with BIS investigation
- Assistance to other BIS investigations
- No previous record of violations

Aggravating factors include:

- Deliberate attempt to hide or conceal violations
- Serious disregard for export compliance responsibilities

[82] Department of Justice, "Summary of Major US Export Enforcement, Economic Espionage, Trade Secret and Embargo-related Criminal Cases (January 2007 to the present" February 2013, p.2 http://www.pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet022013.pdf

[83] Bureau of Industry and Security, Office of Congressional and Public Affairs, "Texas Company to Pay $100 Million for Export Violations to Iran, Syria, Cuba, and Other Countries", 26 November 2013http://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/102-about-bis/newsroom/press-releases/press-releases-2013/603-texas-company-to-pay-100-million-for-export-violations-to-iran-syria-cuba-and-other-countries

[84] See Supplements 1 and 2 to Part 766 EAR

- Involvement of particularly sensitive items or reason for control
- History of violations
- High quantity of value of export[85].

When determining corporate liability at the end of an investigation, a key element will be whether the company has taken the necessary measures and performed meaningful risk analysis.

Federal prosecutors are obliged under the Principles of Federal Prosecution of Business Organisations to consider, among the factors, **the existence of effective compliance programs**. However, in *United States v. Potter* case, it has been stated that a corporation cannot "*avoid liability by adopting abstract rules*" that forbid its agents from engaging in illegal acts, because *"even a specific directive to an agent or employee or honest efforts to police such rules do not automatically free the company for the wrongful acts of agents*"[86].

Critical is therefore the ability to **prove the existence and effectiveness of internal compliance standards**, as set by an accessible and easy-to-read code of business conduct.
In order to make sure these policies are followed and enforced, written procedures and protocols will have to address issues like the timely update of changes in export classification or sanctioned destinations, or how to report potential violations. The company will also need to ensure adequate and regular training for employees and recordkeeping requirements, together with internal and external reviews of audits.

A key role is played by compliance officers, especially local managers as they are best situated to identify risks before they become violations. In 1991, implementation of the Business Organisations section of the United States Sentencing Guidelines Manual highlighted the possibility to obtain penalty reductions if a company could prove to have effective compliance and ethics programs that entailed clear reporting lines and a structured authority of the chief compliance officer[87]. In *2010 US Sentencing Guidelines*, the US Sentencing Commission stressed again the relevance of compliance officers and accountability, highlighting **the importance of giving chief compliance officers direct access to the board of directors**. [88]

In most cases Commerce and State Department enforcement agencies reach negotiated settlements prior to a formal administrative hearing, as a result of "**Voluntary Self-Disclosures**" (VD) of violations made by companies and individuals. VDs are letters by

[85] Bureau of Industry and Security, U Department of Commerce, *Don't Let This Happen To You, An Introduction to US Export Control Law", cit.*
[86] 463 F.3d 9 United States of America, Appellee, v. Nigel Potter; Daniel Bucci; and Lpri, Llc, F/k/a Burrillville Racing Association, A/k/a Lincoln Park, A/k/a Lincoln Greyhound Park, A/k/a Lincoln Park, Inc., Defendants, Appellants. United States Court of Appeals, First Circuit. - 463 F.3d 9, Heard August 2, 2006 Decided September 8, 2006, available online http://law.justia.com/cases/federal/appellate-courts/F3/463/9/621977/
[87] See P.A. Tuffin, "Effective Compliance and Ethics Programs Under The Amended Sentencing Guidelines", American Bar Association, Business Law Section, Summer 2010, http://apps.americanbar.org/buslaw/committees/CL925000pub/newsletter/201007/
[88] United States Sentencing Commission, *2010 Federal Sentencing Guidelines Manual,* http://www.ussc.gov/Guidelines/2010_guidelines/ToC_HTML.cfm

which a company or an individual declare to be responsible for what they believe might be a violation of the regulations.
Since they represent an indicator of the will to comply with export control requirements and may provide the competent agencies with relevant information on other violations, Voluntary Self-Disclosures are considered as a mitigating factor of "great weight" in the negotiation of settlements, and generally lead to significant reduction of fines and other administrative penalties.

4. The Export Control Reform (ECR)

US export controls are undergoing significant revisions as a result of the **Export Control Reform (ECR) Initiative**, initiated by President Obama in 2009.

The Initiative essentially responds to American companies, notably industries dealing with aeronautics and space, that have been long demanding a whole new approach to export controls. The present system has been accused to be a Cold War relic, grounded on the perceived threats and commercial technologies of the time and therefore unable to fit the era of global markets, anachronistic, obsolete and counterproductive.

Allegations have pointed out that export control problems have affected business relations with allies and partners, and even contended that lack of adequate revision and update of the regulations would lead to an increasing risk for national security[89]. **Some peculiar features** have been identified, that would be responsible for an essential disadvantage for American companies:

- The **bureaucratic burden** and complex licencing regime
- The **treatment of some dual use items** as munitions
- The existence of **controls on re-exports**
- The **enforcement of controls on US-owned foreign entities and foreign products** derived from US technology or embedding US components.

American companies also lamented the **costs of compliance**. Besides the costs of setting effective standards of compliance, every year manufacturers and exporters of defence-related commodities are subject to annual registration requirements and fees. Any firm engaged in manufacturing, exporting or brokering any item on the USML must register with the DDTC and pay a yearly fee, ranging between 2250$ and 2750$, whether or not it seeks to export during the year[90].

The Initiative includes broader changes than any of the previous attempts, an interagency review of the whole US export control system, to be carried out in a comprehensive effort of **simplification and rationalisation**. Its stated priorities are:

- Focusing resources on the threats that matter most, *i.e.* allow exports of less critical items under less restrictive conditions and "**build higher walls**" around more sensitive items

- Increase **interoperability** with allies

- Strengthen the US defence industrial base and **enhance competitiveness** by reducing incentives for foreign manufacturers to avoid using US parts and components.

[89] The American Institute of Aeronautics and Astronautics (AIAA), "Lessening the Impact of Export Controls on the US Aerospace Industry, An AIAA Information Paper", http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/National_Security/Export%20Controls-%20030112.pdf

[90] I. F. Fergusson, Paul K. Kerr, "The US Export Control System and the President's Reform Initiative", *cit.*, p.6

In the ECR vocabulary, "**simplification**" is the key word. In April 2010, Secretary of Defence Robert Gates summarised the four main points of the reform:

- A **single licencing agency** for dual use, munitions exports and treasury administered embargoes
- A **unified control list** for items subject to varying levels of restrictions
- A **single primary enforcement coordination agency**, and
- A **single information technology infrastructure** to submit and process licence applications, which would include a single database of sanctioned and denied parties[91].

The final result should be a more a streamlined and refined structure, harmonised definitions and clear jurisdiction but also the end of a situation in which no agency knows "collectively" what has been licenced (or denied) by the US government[92].

Three phases have been envisaged, starting from harmonisation of the CCL with the USML ("phase one"), and standardised licencing and enforcement processes ("phase two"). Phase three should mark the creation of the new export control system with the merger of the two control lists, the setting up of a single licencing agency and of one enforcement agency, together with a new operational IT system.

The first steps in the creation of this new system have been focusing on the **rationalisation and harmonisation of the control lists**. On April 2013, "Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform" were finally published on the Federal Register, to take effect on 13th October 2013.

In this phase, tens of thousands of items, mostly parts and components, are being moved from the USML to CCL.
According to the US Administration, at the end of the reform process, the USML shall contain "*only those items that provide at least a significant military or intelligence applicability that warrant the controls the AECA requires*"[93].

A new ECCN was established for items migrating from the jurisdiction of State to Commerce, or **"600" series ECCNs**: the name derives from the third character on the ECCN (e.g. 9A**6**10). The items affected by this rule are especially aircraft, gas turbine engines, and related items.

[91] I. F. Fergusson, Paul K. Kerr, *cit.*, p.1.
[92] I. F. Fergusson, Paul K. Kerr, *cit.*, p.11.
[93] Remarks of BIS Assistant Secretary for Export Administration Kevin Wolf to the Update 2011 Conference, Washington DC, 19 July 2011.

USML Categories subject to revision included notably VIII (Aircraft), XIX (Gas Turbine Engines), XVII (Classified Articles and Technical Data), and XXI (Miscellaneous Articles). New "600 series" ECCNs became effective on 6th January 2014, for military vehicles, vessels of war, submersible vessels, oceanographic equipment, related items, and auxiliary and miscellaneous items.

These items will be subject to stricter controls than the other items of the CCL, and generally subject to a general policy of denial to countries in the Country Group D:5, that are subject to a US or UN embargo[94].

The STA Exception (**Strategic Trade Authorisation)** destined to "low risk" countries, will be applicable to 600 series only after a determination made jointly by the State, Defence and Commerce Departments[95].

The proposed rules also covered **"transition" rules**, for instance to eliminate the need to obtain authorisation from both BIS and DDTC for a single export, and the key definition of "specially designed", a "catch-all" notion which did not have the same meaning under State and Commerce Departments[96].

The reform will be very comprehensive, however the objective is ambitious. The move of items from the jurisdiction of the State Department to Commerce will simplify administrative burden for US companies dealing with these categories, while others complain that they will still face the "ITAR taint" as they are trading items that are not included, like space or night vision.

On the other hand, it is not completely clear whether it will make life easier for non-US exporters.

As a result of the creation of 600 series ECCN, exporters and re-exporters will de facto need to consider an additional list, new definitions like the one of "specially designed" will need face the test of practice and complex paperwork will be associated to Licence Exception STA. Although there is no "see through rule" in EAR, in certain cases control will extend to foreign made items located outside the US as a result of the *de minimis* and direct product rules.

---

[94] While the 25% *de minimis* rule will apply also to 600 series, no *de minimis* will apply to embargoed destinations. EAR § 740.2(a)(13) lists the EAR License Exceptions available for "600 series" items. For U.S. arms embargoed countries, license exceptions will not be available except a narrow part of License Exception GOV, which is for U.S. government personnel. Other restrictions will apply under Section 740.2, for instance, for missile technology, a license exception will be available only in few cases, and there are also restrictions in each specific section of each applicable license exception.

[95] Starting on 15 October 2013, STA allows export of less sensitive military items without a licence to 36 countries including NATO partners and members of the multilateral non-proliferation regimes.

[96] (1) As a result of "development" has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant ECCN or U.S. Munitions List (USML) paragraph; or (2) Is a "part," "component," "accessory," "attachment," or "software" for use in or with a commodity or defense article 'enumerated' or otherwise described on the CCL or the USML. See "Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform," 78 Federal Register 22660, April 16, 2013; "Revisions to the International Traffic in Arms Regulations: Initial Implementation of Export Control Reforms," 78 Federal Register 22740, April 16, 2013.

The record of public comments (from companies worldwide) on the proposed rule is very indicative of the multiple concerns that the new provisions have been raising.
In general Universities, companies and Industries 'associations in the US have expressed support for the transfer of items from the USML to CCL, hoping that this will effectively lead to controls that apply only to items that provide the US with a critical military or strategic advantage.

However concerns remain, especially for spacecraft-related items. Fear for greater need for "deemed export" licences could result from the definition of "use" included in Part 772.1 EAR.

5. The European perspective

While American industries have been complaining about competitive disadvantage and losses of market shares and lobbying to obtain a reform, European industries business investments and initiatives continue to be very dependent on American export control regulations.

In the Old Continent, international business activities need to comply with a **multi-layered set of regulations**: laws and regulations of the country in which they are established, applicable European Regulations, the law of the respective countries of suppliers and subcontractors and eventually the laws of the country of the client[97]. In this context, American export controls represent **an additional burden for European companies**.

It has already been pointed out how, as a result of **theories of extended jurisdiction**, US export controls affect any company that integrates, resells or manufactures commodities using US origin products, components or technology. However, such invocation of jurisdiction cannot be justified by any legal bases in international law.

No specific rules of international law govern the nationality of goods other than aircrafts or ships. The concept of "nationality" in itself is regarded as a fundamental human right and was in itself developed almost exclusively for persons. Several courts thus rejected US jurisdictional claim and refused to recognise the right to prohibit the export of goods situated on the territory of another country. In the *American President Lines* case, the Supreme Court of Hong Kong found that once discharged, the *lex situs* should apply to commodities present on the territory of Hong Kong and that any attempt to exercise US jurisdiction would be "an incursion into the sovereign rights" of the State[98].

In fact the European Commission expressed concern *vis-à-vis* the extraterritorial impact of third countries already in the 80s. In 1982, the Legal Service of the Commission judged the extraterritorial outreach of certain amendments to the American EAA as not in accordance with international law[99].

EU Regulation No 2271/96 and Joint Action 96/668/CFSP were enacted with these principles in mind. Regulation No 2271/96, in particular, stated that whenever a person's economic and/or financial interest are affected by the extraterritorial application of

[97] With an eye to "soft laws" like the European Union Code of Conduct on Arms Exports and the EU Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment. On the costs and implications of a multi-layered export control regulatory framework, See "Industry's Changing Role in Ensuring Export Control Compliance: Intangible Technology Transfers and Extraterritorial Requirements" in *European Dual-Use Trade Controls: Beyond Materiality and Borders"*, Brussels, P.I.E. Peter Lang, Non-Proliferation & Security, No 8, 2013, p. 45.

[98] American President Lines v. China Mutual Trading Company, 1952 A.M.C. 1510, 1526 (Hong Kong Supreme Court) See also Moens v. Ahlers North German Lloyd, 30 R.W. 360 (Tribunal of Commerce, Antwerp 1966).

[99] See the "Comments on the European Community on the Amendments of 22 June 1982 to the Export Administration Act", Presented to the United States Department of State, 12 August 1982, Paragraph 10. See also O. Jankowitsch-Prevor, Q. Michel, "National Responses", in: *European Dual-Use Trade Controls : Beyond Materiality and Borders"*, Brussels, P.I.E. Peter Lang, Non-Proliferation & Security, No 8, 2013, p.38.

legislation adopted in a third country, the Commission shall be informed within 30 days from the date on which such information was obtained[100].
However, in 1997, EU and US reached an agreement and the effects of this regulation were essentially "frozen". As a result, at present **the EU legal system does not contain, neither at European or Member State's level, any specific provision** to counter extraterritorial effects in the field of export controls[101].

From the point of view of exporters, however, compliance with US regulation is **inevitable**: corporate interests want and need to ensure unfettered access to international markets, avoid sanctions, protect their businesses. In fact, the US can effectively lever on its political influence and economic importance, as no country or company wants to be proscribed by such an essential market.

In the most recent years, the enforcement of American export controls has focused more and more on cases that involve **non-US individuals and companies**. The main target has probably been financial institutions, as they play a very central role in trade-related transactions. In 2012, ING Bank N.V., headquartered in the Netherlands, was accused of movements of capitals reaching the sum of 2 billion $ between 1990s and 2007 through the US financial system on behalf of sanctioned Cuban and Iranian entities. ING agreed to pay 619 million $, the largest fine ever imposed for violation of US sanctions laws. Not much less had had to pay in the previous years ABN AMRO Bank N.V., now Royal Bank of Scotland (RBS)($500 million, 2010), Barclays Bank ($298 million, 2010), Credit Suisse ($536 million, 2009), and Lloyds TSB Bank ($350 million, 2009)[102].

Private entities have also witnessed that US export control violations not only can lead to severe fines and criminal or civil sanctions, but also **to loss of market shares, ban from receiving any US items, and important reputational damage** both for companies and managers. In 2012, French aeronautics spare parts company Aerotechnics France was accused to have illegally exported US military items to Iran: the names of the company and of its CEO were added to the Entity List. When a new company was created from it, with a new managerial board, the Commerce Department evidenced a direct nexus with the previous company and listed the new firm and CEO as well. Only more recently the names were finally taken off the list[103]. More recently, on January 2013, British businessman Christopher Tappin was sentenced 33 months of prison and a fine of 11357$ for the illegal

[100] Under its art. 11 the Regulation applies to "1. Any natural person being a resident in the Community (4) and a national of a Member State, 2. any legal person incorporated within the Community, 3. any natural or legal person referred to in Article 1 (2) of Regulation (EEC) No 4055/86 (5), 4. any other natural person being a resident in the Community, unless that person is in the country of which he is a national, 5. any other natural person within the Community, including its territorial waters and air space and in any aircraft or on any vessel under the jurisdiction or control of a Member State, acting in a professional capacity". Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, Official Journal L 309, 29/11/1996, p. 0001-0006.
[101] O. Jankowitsch-Prevor, Q. Michel, "National Responses", *cit.,* p.39
[102] As reported by Steptoe & Johnson LLP, Edward J. Krauland, Jack R. Hayes, Shannon P. MacMichael, Elisabeth Page, Meredith A. Rathbone, Julia Court Ryan, Maury Shenk and Guy Soussan, "United States: ING Bank To Pay $619 Million Fine In Largest Ever US Economic Sanctions Penalty, 29 June 2012, http://www.mondaq.com/unitedstates/x/184076/Export+controls+Trade+Investment+Sanctions/ING+Bank+to+Pay+619+Million+Fine+in+Largest+Ever+US+Economic+Sanctions+Penalty
[103] See Department of Commerce, Bureau of Industry and Security, *Addition of Certain Persons to the Entity List* and *Implementation of the Entity List Annual Review Changes,* Federal Register Volume 77, No 25, April 2012.

export of defence articles in connection with efforts to export to Iran components of the Hawk Air Defence Missile.

When dealing with items or technology that are controlled under US export control laws, it is therefore important that European exporters know that compliance obligations might be attached, fully understand the regulations and set up effective compliance programs. The ongoing reform in the United States can be in this sense an opportunity "to catch-up" for European exporters.

However, it is still hard to say if the reform will be really beneficial to non-US entities. In the short term the reform will be burdensome and costly for exporters, and will certainly entail additional work.
While the stated objective is to make export control rules more straightforward and less burdensome, administrative burden is to be reduced-in the long term-at the cost of rules that are very likely to be more difficult to understand and administer[104].

[104] Gary Stanley, "The Politics of Export Control Reform: Why Less Licencing = More Complexity", 15 August 2013, http://nextlabs.wordpress.com/2013/08/15/the-politics-of-export-control-reform-why-less-licensing-more-complexity/

6. Conclusions

Export controls are an essentially political tool, designed to foster US national security and foreign policy, but also national commercial interests.

In the United States, national security is intimately intertwined with trade promotion and restriction.
Encouraging more businesses to export "safely" overseas is an essential measure to maximise economic and national security benefits of international trade. As US Under Secretary of Commerce William Reinsch said, US export control policy is now "*based on the reality of economic globalization and the realization that, as a result, our national security is a direct function of our economic health and security*"[105].

Overseas, the equation between trade and security also imposes national restrictions and controls, and leads States to participate into multilateral engagements or regional efforts. Even if a theory of extraterritorial application of American regulations has been questioned, in practice European businesses face a multi-layered set of compliance obligations when dealing with strategic or defence-related commodities or information: national obligations, European directives and regulations, but also US laws and regulations.

The global relevance of the US market, its technological edge and economic power *de facto* allow the possibility to impose conditions on "US-originated" exports.
The American market is still the most important for high technology and defence-related commodities, and companies operating in this field cannot afford having it precluded. Through the years, foreign companies have created and refined their compliance procedures with US regulations, sent regular Voluntary Disclosures and eventually negotiated sanctions.

European companies that want to access this market and trade in strategic, "dual use" or military items need to include "US export control reasoning" in their procedures, in addition to their national obligations. US Licence holders will also need to understand and comply with licence conditions, maintain records, communicate conditions to employees that have access to the items and avoid contamination effects.

While the Export Control Reform (ECR) Initiative is slowly yet substantially changing the compliance regulations and enforcement scenario, the number of actors that need to comply with American regulations is drastically increasing and adopting effective and updated procedures is necessary more than ever.

In this sense, although without any pretention to being exhaustive, this handbook wants to be a useful tool, a reference and a guide to get to know the applicable legal texts, understand their rationale, and effectively manage compliance obligations.

[105] W. A. Reinsch, "Export Controls in the Age of Globalization", The Monitor: Nonproliferation Demilitarization and Arms Control 5 (Summer 1999), p.3, M. Beck, "Reforming the Multilateral Export Control Regimes", *cit.*