

# ITAR FOR GOVERNMENT CONTRACTORS

## Revised For Recent Amendments



[WILLIAMSMULLEN.COM](http://WILLIAMSMULLEN.COM)

**WILLIAMS  
MULLEN**  
findingyes®

# WILLIAMS MULLEN

Thomas B. McVey  
Direct Dial: 202.293.8118  
[tmcvey@williamsmullen.com](mailto:tmcvey@williamsmullen.com)

## **ITAR FOR GOVERNMENT CONTRACTORS**

### **Revised For Recent Amendments**

By: [Thomas McVey](#)<sup>1</sup>  
Williams Mullen

August 8, 2017

### **Table of Contents**

A. Is My Company Subject To ITAR?.....	2
B. Export Administration Regulations – Companion Controls Under Recent Amendments.....	7
C. Specialized ITAR Requirements For Government Contracts Firms. ....	9
D. Compliance Strategies For ITAR/EAR Compliance.....	14

**Introduction.** One of the most important areas of regulation for defense contractors is the International Traffic In Arms Regulations (ITAR). ITAR are the State Department controls that regulate the defense industry.<sup>2</sup> Companies regulated under ITAR are subject to a number of requirements including registration, licensing, restrictions on transferring controlled technical data and performing defense services, among others. Following recent amendments, a second set of regulations - the Export Administration Regulations (EAR)<sup>3</sup> - impose related requirements for government contracts firms and must be considered alongside ITAR. Contrary to popular belief, these apply beyond export transactions to many domestic activities of U.S. defense firms

---

<sup>1</sup> Thomas B. McVey is the Chair of the [International Practice Group](#) of Williams Mullen, where he practices in the areas of ITAR, EAR and the federal regulation of international business. Additional articles on ITAR, EAR and US sanctions programs are available at "[ITAR Articles.](#)" Mr. McVey coordinates closely with the Williams Mullen Government Contracts Practice Group, Co-Chaired by Tony Anikeeff and Robert Korroch.

<sup>2</sup> The ITAR can be found at 22 CFR Chapter I, Subchapter M, Parts 120-130.

<sup>3</sup> The EAR can be found at 15 CFR Chapter VII, Subchapter C.

# WILLIAMS MULLEN

- they can apply even if the company's only customer is the U.S. Government. Due to the potential civil and criminal liability involved, it is imperative for defense firms to have a clear understanding of these laws. The following provides an overview of these requirements and strategies for complying with them.

## A. Is My Company Subject to ITAR?

(1) The U.S. Munitions List. At the core of the ITAR is a list of products called the U.S. Munitions List (USML). The USML contains a wide array of products as well as software, technical data and services. If a company's product, software, technical data or services are identified on the list, the company is subject to the ITAR requirements.

The USML contains twenty-one broad categories of products, ranging from firearms and military vehicles to computers and communication equipment. The original intent behind these regulations was to list military products, however over time the USML has expanded to cover many items that are used in both military and commercial applications. Examples of items covered on the USML are:

- Specified command, control and communications systems including certain radios (transceivers) and identification equipment;
- Military training services and equipment;
- Certain types of drone aircraft;
- Body armor providing protection level equal or above NIJ Type IV;
- Inertial navigation systems specially designed for military aircraft;
- Military vehicles and certain specially designed parts and components;
- Naval vessels and certain specially designed equipment, parts, technologies and software;
- Certain satellites, launch vehicles and ground control equipment, including parts, technologies and software;
- Certain electronic sensor systems;
- Advanced materials such as ablative materials fabricated from advanced composites;
- Specified lasers and related systems;
- Certain underwater sound equipment;
- Certain flight control, radar, avionics products, software and technologies;
- Classified products, technical data and software;
- Toxicological agents; and
- Certain auxiliary military equipment.

A complete list of the 21 Categories covered on the USML is attached below in Exhibit A.

If a company's product is on the USML, the company is subject to a number of requirements in domestic and international activities, as more fully described below.

# WILLIAMS MULLEN

(2) Regulation of Technical Data and Software. ITAR covers not just products, but also software and technical data as well. If an item is listed on the USML, software required to run that item is typically also covered on the USML. Similarly, technical data related to the item is also usually listed on the USML. Technical data is defined to include information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of articles on the USML.<sup>4</sup> If a company produces any of these items it is subject to ITAR.

(3) Services. In addition, the ITAR covers “defense services.” If an item is listed on the USML, the performance of many types of services related to such item for foreign parties are also covered on the USML and subject to ITAR. This includes services involving the installation, design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. In addition, providing military training to foreign parties as well as “military advice” to such parties are considered defense services subject to ITAR. Even if a company does not manufacture or sell a particular product that is listed on the USML, if it performs services related to such items the services may be covered under the USML and the company subject to ITAR.

(4) Parts and Components. The USML covers not just end-products but also subsystems and certain parts, components, accessories, attachments and software that are “specially designed” to be used with end- items on the USML. (In addition, many “specially designed” parts and components of ITAR items are regulated under the EAR – see Section B below). Under the State Department’s interpretative “See-Through Rule,” if a part or component is subject to ITAR and used in a larger system, the *entire larger system* becomes subject to ITAR regulation. This creates significant complications for both U.S. and foreign companies that supply defense components including second- and third-tier suppliers. Thus, these controls reach far and wide within the defense supply chain.

(5) Products and Technologies Developed From Government Research Funding. A key factor that the State Department considers in assessing if a product is on the USML is whether the product or technology was originally developed from U.S. Government funding. Many products that were developed using U.S. defense research funding, such as under SBIR contracts or DOD research grants, are on the USML and hence the product, as well as the technical data, software and defense services related to such product, may be ITAR-controlled.

(6) Universities and Research Institutions. ITAR applies beyond commercial firms to universities, research institutions and other not-for-profit organizations involved in technology research and development. Indeed, some of the most important technologies in the defense field are being developed in these institutions and ITAR

---

<sup>4</sup> Information that is in the “public domain” as defined in 22 CFR §120.11 is not considered controlled technical data. In addition, certain additional types of information are outside the scope of “technical data” – see 22 CFR §120.10(b).



# WILLIAMS MULLEN

controls apply within these as well. In one well known case, a professor at the University of Tennessee was sentenced to four years in prison for ITAR violations related to the disclosure of ITAR-controlled technical data to foreign national students in his laboratory at the University.<sup>5</sup>

(7) Obligations Under ITAR. If a company's products, software, technical data or services are on the USML, ITAR imposes a number of requirements and the company may become subject to one or more of the following unless a license exemption applies:

- Registration – If a U.S. company manufactures, exports, temporarily imports or brokers an item on the USML or performs a “defense service” the company is required to register with DDTC under ITAR Part 122. Note that registration is required even if a company only performs domestic manufacturing activities – exporting is not required to trigger the registration obligation.<sup>6</sup>
- Transfer of Technical Data and Software to Foreign Nationals – The company is prohibited from transferring software or technical data on the USML to foreign nationals,<sup>7</sup> either in the U.S. or abroad, without an export license, unless a license exemption applies. This applies even if the foreign national is an employee of the company.
- Defense Services – The company is prohibited from performing “defense services” related to items on the USML for foreign parties, either in the U.S. or abroad, without obtaining a State Department authorization called a Technical Assistance Agreement (TAA).
- Export License – The company is prohibited from exporting products listed on the USML without obtaining an export license unless a license exemption applies.
- Reexports/Retransfers – If an ITAR-controlled item is exported under a license, the foreign recipient is not permitted to reexport the item (i.e., export the item to another foreign country) or retransfer the item (i.e., transfer the item to another party or for a different end use in the same foreign country) unless the State Department has provided specific authorization for the reexport/retransfer.
- Products Manufactured Abroad Using ITAR-Controlled Items – If a foreign party uses an ITAR-controlled component in a new product manufactured abroad, or

---

<sup>5</sup> See <https://www.fbi.gov/knoxville/press-releases/2012/former-university-of-tennessee-professor-john-reece-roth-begins-serving-four-year-prison-sentence-on-convictions-of-illegally-exporting-military-research-data>

<sup>6</sup> While there are a number of exemptions from the registration requirement as set forth in 22 CFR §122.1(b), if a company is exempt from the registration requirement it may still be subject to many of the other requirements under ITAR.

<sup>7</sup> A “Foreign Person” is defined in ITAR §120.16 as a person who is not a US citizen, permanent resident alien (green card holder) or “protected individual” under 8 USC §1324b(a)(3), or is a foreign business entity that is not incorporated in the US.

# WILLIAMS MULLEN

manufactures a new foreign product based upon ITAR-controlled technical data, the new product manufactured abroad becomes ITAR-controlled. As such, the foreign party is not permitted to transfer the foreign produced item to any other parties unless DDTC provides specific authorization for such transfer. If a US company grants a foreign party an authorization to manufacture defense articles abroad which involve the use of ITAR-controlled technical data, the parties are typically required to execute a Manufacturing License Agreement (MLA) which has been authorized by DDTC and comply with other requirements. In addition, agreements between U.S. companies and foreign companies for the warehousing and distribution of defense articles overseas (referred to as Warehousing and Distribution Agreements) must be approved in advanced by the Directorate of Defense Trade Controls (DDTC).

- Temporary Imports – The company is prohibited from importing defense items listed on the U.S. Munitions List in temporary import transactions without obtaining a temporary import license<sup>8</sup>.
- Brokering – If companies perform activities to assist or facilitate the sale of ITAR-controlled items to non-US parties this is generally referred to as “brokering activity.”<sup>9</sup> Parties who engage in brokering activities are subject to numerous requirements including broker registration, the requirement to obtain advanced State Department authorization to perform brokering activities for certain products, reporting, recordkeeping and restrictions on engaging in brokering transactions involving the Section 126.1 “Proscribed Countries” (See Section C.(4) below).
- Reports for Payments of Sales Commission, Fees and Political Contributions – Companies that pay sales commission, fees and/or political contributions in connection with the sale of ITAR-controlled products or services that meet the requirements of ITAR Part 130 are required to file reports with DDTC regarding such payments and comply with other requirements under ITAR Part 130.
- Transactions With Debarred Parties – Persons who have been debarred or who are deemed “ineligible” under the provisions of ITAR §120.1(c)(2)<sup>10</sup> are prohibited from entering into transactions regulated under ITAR. In addition, companies are

---

<sup>8</sup> In addition, parties that import items on the US Munitions Import List in permanent import transactions will be subject to regulations promulgated by the Bureau of Alcohol, Tobacco, Firearms and Explosives.

<sup>9</sup> The definition of “brokering activities” is set forth at ITAR §129.2(b).

<sup>10</sup> ITAR §120.1(c)(2) provides as follows: Persons who have been convicted of violating the U.S. criminal statutes enumerated in §120.27, who have been debarred pursuant to part 127 or 128 of this subchapter, who are subject to indictment or are otherwise charged (e.g., charged by criminal information in lieu of indictment) with violating the U.S. criminal statutes enumerated in §120.27, who are ineligible to contract with or to receive a license or other form of authorization to import defense articles or defense services from any agency of the U.S. Government, who are ineligible to receive an export license or other approval from any other agency of the U.S. Government, or who are subject to a Department of State policy of denial, suspension, or revocation under §126.7(a) of this subchapter, are generally ineligible to be involved in activities regulated under the subchapter.

# WILLIAMS MULLEN

prohibited from entering transactions regulated under ITAR if other parties involved in such transactions have been debarred or are otherwise ineligible under §120.1(c)(2).

- §126.1 Proscribed Countries – Companies are prohibited from (i) entering transactions regulated under ITAR involving countries listed in ITAR §126.1 (referred to as the “Section 126.1 Proscribed Countries”) without specific DDTC authorization (which is subject to a policy of denial); (ii) submitting marketing proposals or presentations to parties in the Section 126.1 Proscribed Countries without advanced authorization from DDTC; and (iii) engaging in brokering transactions with parties involving the Section 126.1 Proscribed Countries. In addition, if a person knows or has reason to know of a proposed, final or actual sale, export or other transfer of ITAR-controlled items involving the Section 126.1 Proscribed Countries they are required to immediately inform DDTC of such event.
- Recordkeeping Requirement – The company is required to maintain records in accordance with the ITAR recordkeeping requirements set forth at 22 CFR §122.5.

(8) Domestic Versus International Activities. Many executives view ITAR to be part of the U.S. export control laws and regulate just exports. However, ITAR regulates a wide variety of activities in purely domestic commercial activity, such as:

- The prohibition of the transfer of technical data or software subject to ITAR to foreign nationals in the United States;
- The prohibition of the performance of defense services for foreign parties in the United States;
- The requirement for U.S. companies to register with the State Department as a domestic manufacturer, even if they do not export any products;
- The requirement to comply with ITAR recordkeeping requirements;
- The requirement to obtain import authorization for the import of defense items; and
- The prohibition of the transfer of USML products to representatives of foreign governments and military organizations (including NATO, United Nations, etc.) in the United States unless a license is obtained or an exemption applies.

(9) Obligations on Foreign Companies. ITAR requirements may also apply to foreign companies including foreign government contractors. For example, if a foreign company receives an ITAR controlled item overseas, including hardware, technical data or software, it is prohibited from reexporting or retransferring such item unless the State Department has provided specific authorization (referred to as reexport or retransfer authorization). Also, as mentioned above, if an ITAR-controlled component is exported from the U.S. and incorporated into a foreign-manufactured product, under the “See-Through Rule” the entire foreign-made product becomes subject to ITAR regulation.

# WILLIAMS MULLEN

(10) Penalties. Penalties for ITAR violations include civil and criminal penalties, including fines of up to \$1,000,000 per violation and up to 20 years imprisonment.<sup>11</sup> Other sanctions include debarment, denial of export privileges and publication of a press release by DDTC regarding the company's violation.

## B. Export Administration Regulations – Companion Controls Under Recent Amendments.

The Export Administration Regulations (EAR) are administered by the U.S. Department of Commerce. The EAR were originally adopted to regulate commercial and “dual use” products. However, under a series of recent amendments known as “Export Control Reform” a large number of items previously regulated under ITAR were transferred to the EAR and hence the EAR now covers certain military products as well. Consequently, contractors must be cognizant of both ITAR and EAR in their compliance activities.

(1) CCL-Based Controls. The EAR contain a list of products called the Commerce Control List (CCL). If an item is listed on the CCL it may be subject to export licensing and other controls depending upon the country to which it will be exported and other factors (these requirements are referred to as the “CCL-Based Controls”). Military products that were transferred from ITAR to EAR jurisdiction under Export Control Reform are listed on the CCL under the newly established “600 Series.”

As with ITAR, the EAR applies not just to physical products but also technology and software as well. The term “technology” is defined broadly at 15 CFR Part 772 as “specific information necessary for the development, production, or use of a product.”<sup>12</sup> Thus if technology or software is on the CCL, there may be restrictions on exporting such items out of the U.S. and disclosing such items to foreign nationals in the U.S.

The requirements under the CCL-Based Controls are similar to many of the requirements under ITAR, including the requirements to obtain export licenses for the export of certain products, restrictions on the transfer of controlled technology and software (including transfers to foreign nationals in the United States or overseas), restrictions on reexports of U.S.-origin products and the incorporation of U.S. components into items manufactured abroad that contain above a *de minimis* level of US content, and restrictions on the performance of services related to weapons of mass destruction and other restricted activities.<sup>13</sup>

---

<sup>11</sup> See: 4th Circuit Lowers Threshold For Criminal Violations Of ITAR at <http://www.williamsmullen.com/news/4th-circ-lowers-threshold-criminal-violations-itar>.

<sup>12</sup> Effective September 1, 2016 the definition of “Technology” set forth in 15 CFR Part 772 will be amended to include: “Information necessary for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item....” See Federal Register, Vol. 81, No. 107, June 3, 2016.

<sup>13</sup> The EAR set forth restrictions on certain services performed by U.S. persons at 15 CFR §744.6.



# WILLIAMS MULLEN

Many subsystems, parts, components, accessories and attachments that are “specially designed” for items on the USML or the CCL are listed on the CCL and subject to controls under the EAR. The term “specially designed” has a specific definition that was adopted as part of Export Control Reform and parties need to apply the “specially designed” definition in interpreting ITAR and EAR.<sup>14</sup>

(2) Broad “Catch-All” Provisions For Many Products and Components Specially Designed For Military Use. As referenced above, under Export Control Reform a significant number of defense items were transferred from the USML onto the CCL and are now regulated under the EAR. As a result, the CCL now includes many “catch-all” subcategories that were previously listed on the USML – these are broad open-ended designations that cover items that were “specially designed” for military use. One significant example of this new “catch-all” under the CCL is ECCN 3A611.a, which reads as follows:

**3A611 Military electronics, as follows:**

\*\*\*\*\*

a. Electronic equipment, end items, and systems “specially designed” for a military application that are not enumerated or otherwise described in either a USML category or another “600 series” ECCN.

Note to 3A611.a: ECCN 3A611.a includes any radar, telecommunications, acoustic or computer equipment, end items, or systems “specially designed” for military application that are not enumerated or otherwise described in any USML category or controlled by another “600 series” ECCN.

\* \* \*

x. Parts, components, accessories and attachments that are “specially designed” for a commodity controlled by this entry or for an article controlled by USML Category XI, and not enumerated or described in any USML category or another 600 series ECCN or in paragraph .y of this entry.

There are also similarly broad “catch-all” categories for other types of products that are “specially designed for a military application” including computers,<sup>15</sup> telecommunications equipment,<sup>16</sup> radar and acoustic systems,<sup>17</sup> navigation/avionics equipment<sup>18</sup> and aircraft.<sup>19</sup> Hence, many components used in the defense industry are listed on the CCL and it is imperative for defense contractors to be cognizant of these.

(3) Export Requirements for All Export Transactions Subject to the EAR. In addition to the CCL-Based Controls, the EAR contain a number of additional requirements that apply to all export and reexport transactions that are subject to the EAR, even if the item in question is not listed on the CCL. These requirements include

---

<sup>14</sup> The ITAR definition of “specially designed” can be found in 22 CFR §120.41. The BIS definition of “specially designed” can be found at 15 CFR Part 772.

<sup>15</sup> See ECCN 4A611, which directs the reader to ECCN 3A611.

<sup>16</sup> See ECCN 5A611, which directs the reader to ECCN 3A611.

<sup>17</sup> See ECCN 6A611, which directs the reader to ECCN 3A611.

<sup>18</sup> See ECCN 7A611, which directs the reader to ECCN 3A611.

<sup>19</sup> See ECCN 9A610.

# WILLIAMS MULLEN

the prohibition against undertaking exports and reexports to certain embargoed countries,<sup>20</sup> to certain restricted parties<sup>21</sup> and for use in certain prohibited end-uses.<sup>22</sup>

(4) Penalties for Violations. Penalties for violations of EAR are similar to ITAR, *i.e.*, civil and criminal penalties including monetary fines of up to \$1,000,000 per violation and up to 20 years imprisonment.

## C. Specialized ITAR Requirements for Government Contracts Firms.

ITAR/EAR compliance is important for firms that perform work for the Department of Defense (DOD) and other federal agencies including U.S. intelligence agencies, Department of State and the Department of Homeland Security. A significant portion of the products and services provided by contractors for military agencies are listed on the USML or the CCL. As such, companies that deal in such items will be subject to these controls, both in the U.S. and overseas, and contractors must adopt processes in their business operations to comply with them.

(1) DFARS §225.79 and 252.225-7048. DFARS §225.79 provides that it is the contractor's responsibility to comply with all applicable export control laws in performing under contracts for the DOD. The contract clause at DFARS 252.225-7048 states: "The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR." (emphasis added.) In addition, §252.225-7048(e) requires that contractors "flow down" this clause to their subcontractors. The adoption of these provisions is part of the DOD's efforts to alert every DOD contractor to its obligations under ITAR and EAR - contractors are responsible for learning about and complying with these laws in activities performed under their contracts.

Based on these DFARS provisions, many prime contractors are requiring their subcontractors to register with DDTC under ITAR and demonstrate knowledge of the requirements under ITAR and EAR. Many prime contractors are also assessing the capabilities of their subcontractors regarding ITAR compliance – if a prime perceives a weakness in a subcontractor, the prime may be reluctant to hire the subcontractor due to fear of potential liability for the prime in the event of an ITAR violation. Thus strong ITAR compliance can create a significant competitive advantage for second and third tier subcontractors and suppliers who are looking to build close relationships with their prime contractors.

(2) Performing Contracts For U.S. Government Customers. Examples of obligations that arise for companies that provide products and services to U.S. Government customers include:

---

<sup>20</sup> See 15 CFR Part 746.

<sup>21</sup> See 15 CFR Part 744.

<sup>22</sup> See 15 CFR Part 744.

# WILLIAMS MULLEN

- Contractors that produce or hold ITAR-controlled technical data or software are not permitted to disclose such items to foreign nationals, either in the U.S. or abroad – including to foreign national employees of the contractor. Companies must adopt procedures to limit foreign national employees’ access to ITAR-controlled products and technical data. (Under ITAR, if a person is a US citizen or permanent resident alien (ie, has a green card), he/she is considered a “US Person;” if the person is present in the US on a visa, he/she is considered a “Foreign Person.”<sup>23</sup>)
- If a company is exporting products or transferring controlled technical data to DOD customers overseas – the company may be required to obtain an export license or otherwise comply with the ITAR requirements in certain transaction unless an exemption applies. (See the discussion below regarding certain limited license exemptions that may apply in providing products or services to U.S. Government agencies.)
- If in performing a contract for a U.S. government agency a U.S. company performs a service for a foreign party related to an ITAR-controlled item (including a foreign military organization such as NATO or a foreign country’s military agency), or discloses controlled technical data to such party (such as in a joint briefing to a US government official and a foreign military official), the U.S. company may be required to obtain an export license or TAA.
- Companies that provide training, intelligence, security services or military advice to foreign military forces under contracts with the DOD may be required to obtain TAA’s or other license authorizations from the State Department.
- If a U.S. company transfers or discloses an ITAR-controlled product or technical data to a representative of a foreign government in the U.S. (including embassies, diplomatic mission or agencies of a foreign government), this constitutes an export and the company is required to obtain a license unless an exemption applies. Similarly, transferring registration, control or ownership of an ITAR-controlled vessel or aircraft to a foreign person in the U.S. is considered an export and the U.S. company is required to obtain a license.
- One of the most important obligations of companies that create or store ITAR-controlled technical data and software is to create adequate controls within their IT systems to prevent foreign nationals (including company employees) from having access to such items. Most defense contractors create and/or store some form of ITAR-controlled technical data or software in their

---

<sup>23</sup> See 22 CFR §120.15 and 120.16.

# WILLIAMS MULLEN

company IT systems, such as electronic drawings, technical specifications, operating instructions, installation manuals or similar documents. If a foreign national employee logs on to the company's computer system and accesses those materials, this will constitute an ITAR violation unless a license is obtained or an exemption applies. Similar risks arise for access by foreign national IT administrators, foreign based outsourced IT contractors and use of "cloud" resources where controlled data is stored in servers located overseas. Contractors are advised to adopt controls within their IT systems to provide adequate security for access by foreign nationals to controlled information.

- Most defense contractors will be required to register under 22 CFR Part 122.

See also [Legal Checklist For International Defense Transactions](#) and [Export Control Laws For The General Counsel](#).

ITAR and EAR contain certain license exemptions that may reduce compliance obligations in providing products and services for federal government agencies, depending upon the details of the activity involved. For example, ITAR §126.4(a) – the "by and for exemption" – provides an exemption from certain licensing requirements for temporary imports and temporary exports by or for an agency of the US Government for official use by such agency, subject to certain conditions.<sup>24</sup> Other exemptions may also be available.<sup>25</sup> However these exemptions are often narrowly drafted and have detailed conditions and hence do not apply in all instances,<sup>26</sup> Similarly, exemptions often have compliance obligations such as certification and recordkeeping requirements.<sup>27</sup> In addition, the exemptions under ITAR and EAR are different – a company may be able to rely on an ITAR exemption for a certain activity but that exemption may not necessarily apply under EAR. Contractors should use care in reviewing the details of any license exemptions that they intend to rely upon. On May 22, 2015 DDTC issued a proposed

---

<sup>24</sup> If a contractor uses the exemption under §126.4, §126.4(c) provides that the exporter is required to submit an Electronic Export Information (EEI) filing as required under 123.22 and a written statement by the exporter certifying that the requirements under §126.4 have been met and must present these to Customs and Border Protection or the DOD transmittal authority, and a copy of the EEI filing and the written certification statement must be provided to the Directorate of Defense Trade Controls immediately following the export.

<sup>25</sup> See also ITAR license exemptions set forth at 22 CFR §125.4(b)(1), §125.4(b)(3), §125.4(b)(9), §125.4(b)(11) and §125.4(b)(13), and BIS license exceptions set forth at 15 CFR§740.11(b).

<sup>26</sup> Examples of conditions that frequently apply in connection with the use of ITAR license exemptions include that the exemption cannot be used for: (i) transactions involving § 126.1 Proscribed Countries; (ii) exports for which Congressional notification is required (see 22 CFR §123.15); (iii) Missile Technology Control Regime articles; (iv) significant military equipment; (v) exports by persons who are "ineligible" under 22 CFR §120.1(c). In addition, DDTC regularly advises parties that companies must be registered in order to take advantage of most license exemptions.

<sup>27</sup> For example, to claim an exemption for the export of technical data under §§125.4 and 125.5, the exporter must certify that the proposed export is covered by a relevant section of this subchapter, to include the paragraph and applicable subparagraph. Certifications consist of clearly marking the package or letter containing the technical data "22 CFR [insert ITAR exemption] applicable." This certification must be made in written form and retained in the exporter's files for a period of 5 years. For exports that are oral, visual, or electronic the exporter must also complete a written certification as indicated in paragraph (a) of this section and retain it for a period of 5 years. See ITAR §125.6.

# WILLIAMS MULLEN

regulation that would significantly expand the scope of the license exception set forth at 22 CFR §126.4, however this regulation has not yet been adopted in final form as of the date of this article.<sup>28</sup>

(3) Performing Contracts for Foreign Defense Agencies. If a contractor provides products or services to foreign defense agencies, either as a prime or subcontractor, ITAR/EAR requirements will often apply. In such cases, the contractor will be subject to many of the requirements described above under ITAR and EAR, including in connection with the export of hardware, transfer of controlled technical data to foreign parties, performance of defense services, brokering, reporting and recordkeeping requirements, unless exemptions apply. It should be noted that these requirements may apply even if activities are performed solely within the U.S. For example, if a foreign customer hires a U.S. contractor to analyze a defense system that is regulated under ITAR and the contractor performs the analysis in the U.S. and sends the results to the customer overseas, this constitutes a “defense service” that will require a TAA (even if the service is performed in the U.S.). Similarly providing military training or military advice to foreign military forces will most likely require a license or TAA. In many instances providing security, executive protection, intelligence services or other technical services to foreign parties will in many instances require a TAA.

(4) The Section 126.1 “Proscribed Countries.” DDTC maintains a list of countries that are subject to U.S. or U.N. arms embargoes which are subject to heightened export restrictions under ITAR. These countries are set forth in 22 CFR §126.1 and are referred to as the “Section 126.1 Proscribed Countries.” These countries are subject to a State Department licensing policy of denial, i.e., if a U.S. company requests export authorization to engage in a transaction with one of these countries involving ITAR-controlled items, the authorization will be denied except in exceptional circumstances. In addition, U.S. companies are not permitted to submit marketing proposals or presentations involving ITAR-controlled activities to such countries (including their embassies or consulates in the US) or perform brokering activities related to such countries unless the Directorate of Defense Trade Controls (DDTC) has authorized such activity in advance.<sup>29</sup> Under ITAR §126.1(e)(2), if a person knows or has reason to know of a proposed, final or actual sale, export or other transfer of ITAR-controlled items involving one of the Section 126.1 Proscribed Countries they are required to immediately inform DDTC of such event. The list of Section 126.1 Proscribed Countries is amended by DDTC periodically so companies should review the list on a regular basis for changes. Contractors are advised to use a high degree of caution when contemplating dealing with Section 126.1 Proscribed Countries in defense-related transactions.

(5) Contracts With NATO, United Nations and NATO Member Countries. We are frequently asked about the status of NATO, United Nations and NATO Member Countries under ITAR. NATO and the United Nations are considered foreign persons under ITAR and hence U.S. companies are required to comply with ITAR and EAR requirements when entering transactions with such parties, unless a specific exemption

---

<sup>28</sup> See 80 Federal Register 29565, May 22, 2015.

<sup>29</sup> See 22 CFR §126.1(e)(1).



applies. Similarly, the foreign country members of NATO are considered foreign persons and ITAR and EAR controls apply unless a license exemption is available.<sup>30</sup>

(6) Brokering of Defenses Articles. ITAR Part 129 regulates “brokering activities” related to ITAR-controlled items. Brokering is defined generally as assisting or facilitating another party’s activities involving ITAR-controlled items even if the broker is not a principal in the transaction (and even if the broker is not paid in the transaction).<sup>31</sup> Parties that engage in brokering activities are subject to a number of requirements including DDTC registration,<sup>32</sup> obtaining advance authorization for brokering certain defense articles, prohibitions from engaging in transactions with the “Section 126.1 Proscribed Countries,” reporting and recordkeeping.

(7) Foreign Military Sales Contracts. ITAR §126.6(c) provides a license exemption for certain exports under the Foreign Military Sales (FMS) Program. However, in order for the exemption to apply the parties must have entered into a Letter of Offer and Acceptance which meets certain requirements under §126.6(c). In addition, §126.6(c) contains a number of additional conditions and limitations and the exemption does not apply unless all of the conditions are met. Hence in some instances ITAR requirements may apply to U.S. contractors under FMS contracts. Contractors are advised to review the provisions of §126.6(c) carefully to determine if any ITAR requirements apply to their FMS sales.

(8) Cyber-Security, Cloud Computing and Reporting of Cyber-Intrusions. On August 26, 2015, the DOD adopted an Interim Rule that provides updated data security requirements for DOD contractors.<sup>33</sup> Under this regulation, certain DOD contractors that process “covered defense information”<sup>34</sup> in their data systems are required to comply with specified data security requirements set out in the regulation. See e.g., DFARS 204.7300<sup>35</sup> and 252.204-7012. “Covered defense information” includes information that is controlled under ITAR or EAR. Consequently, DOD contractors that are subject to this regulation that process or transmit ITAR-controlled or EAR-controlled technical data or software under their DOD contracts will be required to adopt the data security measures set out in the regulation. The regulation also provides additional requirements including: (i) the requirement for contractors to report cyber-intrusions and malicious software in their data systems to the DOD; (ii) security requirements when using “cloud” computing resources; and (iii) the requirement to “flow down” these requirements to

---

<sup>30</sup> See, e.g., 22 CFR §126.14 and §125.4(c).

<sup>31</sup> The definition of “broker” is set forth at 22 CFR § 129.2(a) and “brokering activities” at 22 CFR §129.2(b).

<sup>32</sup> Registration as a broker under 22 CFR Part 129 is separate from registration as a defense manufacturer or exporter.

<sup>33</sup> See Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Interim Rule, Federal Register Vol. 80, No. 165, August 26, 2015. See also related Interim Rule issued on December 30, 2015: Federal Register Vol. 80, No. 250, December 30, 2015.

<sup>34</sup> See DFARS §204.7301.

<sup>35</sup> See generally DFARS Subpart 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting.

# WILLIAMS MULLEN

certain subcontractors. In a subsequent Interim Rule issued on December 30, 2015,<sup>36</sup> portions of the regulation were subject to a delayed implementation date provided that the contractor provides notification to the DOD as set forth in the rule.<sup>37</sup> Contractors should review their contracts with their DOD customers and consult with their contracting officers to determine the precise data security requirements that will apply to them under their contracts.

## D. Compliance Strategies for ITAR/EAR Compliance.

Due to the complexity of this area of the law, a contractor cannot simply rely on good intentions to avoid ITAR/EAR violations. If a company is subject to these requirements there are a number of steps to take to reduce the risk of violations:

(1) Identify Export Control Requirements That Apply to the Company. The first step is to review the company's business activities to determine the precise ITAR/EAR requirements that will apply to it. Such requirements will vary depending upon the company's business, products it sells, services it performs and countries in which it operates. As part of this the company should review its products and services to determine if they are listed on the USML and the CCL.<sup>38</sup> Based upon this review the company can then identify the exact requirements that apply to it on an ongoing basis. We advise that government contractors review each new contract and task order that they receive to determine in advance if any ITAR/EAR requirements will apply in the performance of the contract.

(2) Adopt an ITAR Compliance Program. The second, and arguably most important step in the compliance effort, is the adoption of an ITAR Compliance Program. This involves the implementation of a formal company-wide effort for complying with ITAR/EAR in the company's day-to-day operations. This includes: (i) the appointment of a company employee to be in charge of ITAR/EAR compliance; (ii) adopting written policies and procedures for your employees to follow in performing activities that are subject to ITAR and EAR; (iii) conducting export compliance training for key employees; (iv) determining the jurisdiction/classification of the company's products and services under the USML/CCL; (v) adopting procedures for screening for prohibited parties, prohibited countries and prohibited end-users; (vi) conducting periodic internal compliance audits; and (vii) adopting a procedure for compliance with the ITAR/EAR recordkeeping requirements.

---

<sup>36</sup> See Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Interim Rule, Federal Register Vol. 80, No. 250, December 30, 2015.

<sup>37</sup> Under the December 30, 2015 Interim Rule, if the contractor is unable to implement these standards at the time of the contract award the contractor is required to notify the Department of Defense, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

<sup>38</sup> The process of reviewing whether a company's products or services are on the USML or CCL is referred to as determining the export jurisdiction and classification of the item.

# WILLIAMS MULLEN

If a company is found to have an ITAR violation, enforcement officials and the courts will often reduce or “mitigate” penalties for companies which have adopted compliance programs, and in some cases, impose no penalties at all.

In many cases companies also conduct compliance audits or similar internal reviews to assess if their activities are in compliance with ITAR/EAR and to identify any past violations. This is typically a confidential internal review conducted by an outside compliance expert or legal counsel.<sup>39</sup> Compliance audits can be an excellent way for companies to identify any weaknesses in their compliance practices in advance and for “cleaning up” any past violations before a government agency does.

(3) Put Your Compliance Practices to Work. Once you have developed the proper expertise and structure within your company for ITAR/EAR compliance, the most important step is to put these into action. This may mean applying for the requisite export licenses, TAA’s and other authorizations, identifying appropriate license exemptions, performing license and TAA administration, reviewing new contracts and task orders for ITAR/EAR requirements and complying with recordkeeping requirements. Proper attention to compliance on an ongoing basis is the best way to eliminate the expense and legal exposure of future violations.

(4) Voluntary Disclosures – Clearing Up Past Violations. An important component of a sound compliance strategy is understanding the use of voluntary disclosures. If a company has discovered a past violation, there are procedures available under ITAR and EAR for the company to voluntarily disclose the violation to the State or Commerce Departments. While mandatory disclosure is not required in most instances, if violations are disclosed before the agency learns about them, this can result in a reduced penalty or in many instances just a “warning letter” with no penalty. In many cases this procedure provides an opportunity to “wipe the slate clean” of past violations if the company commits to improved compliance activities in the future. However, voluntary disclosures must be undertaken prior to the agency learning of the violation or the benefits will not be available to the company.

Taken together, these steps provide the structure and process for a company to undertake a serious effort to protect against ITAR/EAR violations. They also provide a firm foundation for a company’s defense in the event any violations occur in the future.

To contact the author or for a complimentary subscription to the William Mullen ITAR newsletter please contact Thomas McVey at: [tmevey@williamsmullen.com](mailto:tmevey@williamsmullen.com) or 202.293.8118. Additional articles on ITAR, EAR and US sanctions programs are available at: “[ITAR Articles.](#)”

**Please note:** This article contains general, condensed summaries of actual legal matters, statutes and opinions for information purposes. It is not meant to be and should

---

<sup>39</sup> If the review is conducted by or under the direction of the company’s legal counsel, this increases the likelihood that the results will be subject to the attorney client privilege and not required to be disclosed in response to a subpoena in the event there is an investigation.

# WILLIAMS MULLEN

not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel. For more information, please visit our website at [www.williamsmullen.com](http://www.williamsmullen.com) or contact Thomas B. McVey, 202.293.8118 or [tmcvey@williamsmullen.com](mailto:tmcvey@williamsmullen.com). For mailing list inquiries or to be removed from this mailing list, please contact the author at [tmcvey@williamsmullen.com](mailto:tmcvey@williamsmullen.com) or 202.293.8118.

## THE US MUNITIONS LIST

- Category 1: Firearms, Close Assault Weapons and Combat Shotguns
- Category 2: Guns and Armament
- Category 3: Ammunition/Ordinance
- Category 4: Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
- Category 5: Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents
- Category 6: Surface Vessels of War and Special Naval Equipment
- Category 7: Ground Vehicles
- Category 8: Aircraft and Related Articles
- Category 9: Military Training Equipment and Training
- Category 10: Personal Protective Equipment
- Category 11: Military Electronics
- Category 12: Fire Control, Range Finder, Optical and Guidance and Control Equipment
- Category 13: Materials and Miscellaneous Articles
- Category 14: Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
- Category 15: Spacecraft and Related Articles
- Category 16: Nuclear Weapons and Related Articles
- Category 17: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
- Category 18: Directed Energy Weapons
- Category 19: Gas Turbine Engines and Associated Equipment
- Category 20: Submersible Vessels and Related Articles
- Category 21: Articles, Technical Data, and Defense Services Not Otherwise Enumerated