

## THE BASICS OF EXPORT CONTROL FOR IMMIGRATION PRACTITIONERS

by Tien-Li Loke Walsh and Abby Walsh\*

Since the 9/11 terrorist attacks, numerous measures designed to enhance security and streamline visa processing have been implemented. Various government agencies, including the U.S. Department of Homeland Security (DHS), the U.S. Department of State (DOS), the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency have consulted in an extensive and ongoing review of visa issuing procedures. These efforts at data sharing have created increasingly sophisticated government databases. Since then, mandatory visa interviews, biometric collection, and expanded security checks have become the norm and foreign nationals applying for nonimmigrant visas at consular posts often encounter significant delays. To further complicate matters, the focus on foreign nationals and their activities in the United States has generated significant government investigation and enforcement in the overlapping issues of export control, bringing these issues to the forefront of immigration practice.<sup>1</sup>

---

Copyright © 2011 Wolfsdorf Immigration Law Group and True Compliance Group (all rights reserved). Reprint permission granted. Excerpted from “*The Technology Alert List, Visa Mantis and Export Control: Frequently Asked Questions*,” by Tien Li Loke Walsh and USCIS Part 6 Training What You Need To Know Before You Sign by Abigail Caldwell Walsh.

\***Tien-Li Loke Walsh** is a senior attorney with the Wolfsdorf Immigration Law Group in Los Angeles. She graduated from the University of Sydney with a B.A. in political science and history, and received her J.D. from Boston University School of Law. Ms. Loke Walsh has published and spoken on a variety of topics at numerous AILA and NAFSA immigration conferences. Ms. Loke Walsh’s immigration law practice focuses on obtaining visas for professors and researchers, artists and entertainers, athletes, investors, multinational company transfers and professionals in various industries. In addition, Ms. Loke Walsh assists clients with I-9 audits, H-1B audits and corporate compliance policies. Tien Li Loke Walsh can be contacted at [tloke@wolfsdorf.com](mailto:tloke@wolfsdorf.com).

**Abby Walsh** is an attorney and CEO of True Compliance Group, which provides compliance, operations, and legal services to national and international companies, across industry lines. Her niche is helping companies identify, design, and implement practical compliance resolutions including export compliance programs; ITAR/EAR training; classification; policies, procedures and best practices; audits; and human resources and immigration matters. Prior to True Compliance Group, Ms. Walsh was general counsel, secretary, and chief compliance officer for CBOL Corporation, an international aerospace distributor and contract manufacturer, where she was responsible for all legal affairs, export compliance, and related operations. Ms. Walsh was also general counsel of Korn/Ferry International Futurestep, Inc., where she managed a global legal department for an Internet-based executive recruiting firm. She also worked in private practice and as an assistant public defender. She holds a law degree from Loyola University of Chicago and a BA from Hamilton College. She is licensed to practice in Illinois and California. Abby Walsh can be contacted at [abbwalsh@truecompliancegroup.com](mailto:abbwalsh@truecompliancegroup.com).

Tien-Li and Abby are both married to Irishmen from the prolific Walsh clan.

<sup>1</sup> See “Export Controls: Improvements Needed to Prevent Unauthorized Technology Releases to Foreign Nationals in the United States,” Report to Congressional Requesters (Feb. 2011) by the U.S. Government Accountability Office, for an excellent insight into the government’s efforts at identifying and addressing weaknesses in the export control system. The executive branch is currently considering reforms to the U.S.

*Cont’d*

On November 28, 2010, the U.S. Citizenship and Immigration Service (USCIS) published a revised Form I-129, Petition for a Nonimmigrant Worker. The revised version became effective on February 20, 2011. There are a number of changes to the form, but the key change is Part 6, which requires a petitioner seeking H-1B, H-1B1, L-1, or O-1A classification to certify that it has reviewed the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR), made a license determination, and, if applicable, will prevent access to controlled technology or data until an export license is obtained.

The key concepts involved in Part 6 on Form I-129 require familiarity with the following:

- U.S. Department of Commerce [known as the Bureau of Industry and Security (BIS)] and U.S. Department of State, Directorate of Defense Trade Controls (DDTC)
- ITAR and EAR
- Foreign Person
- Technology or Technical Data
- Release (“Export” and “Deemed Export”)
- License determination
- Other authorization for release
- Preventing access to the controlled technology or technical data

These are extremely complex concepts and companies will need training and/or expert advice to answer the questions in Part 6. Many companies are simply unaware of export control requirements, which could expose a company to door-closing criminal, civil, and administrative fines and penalties. Therefore, it is critical to advise your client of the potential export control issues and to refer them to training and/or export compliance counsel. At the same time, it is important for you to have a familiarity with some of basic export concepts.

#### **U.S. Dept. of Commerce [Bureau of Industry and Security (BIS)] and U.S. Dept. of State, Directorate of Defense Trade Controls (DDTC)**

While there is a long list of federal agencies that can be involved in export control, for the purposes of Part 6 on Form I-129, the focus is on the U.S. Department of Commerce—now commonly referred to as BIS.<sup>2</sup> BIS governs commercial and dual-use items and technology, including software and encryption items. The U.S. Department of

---

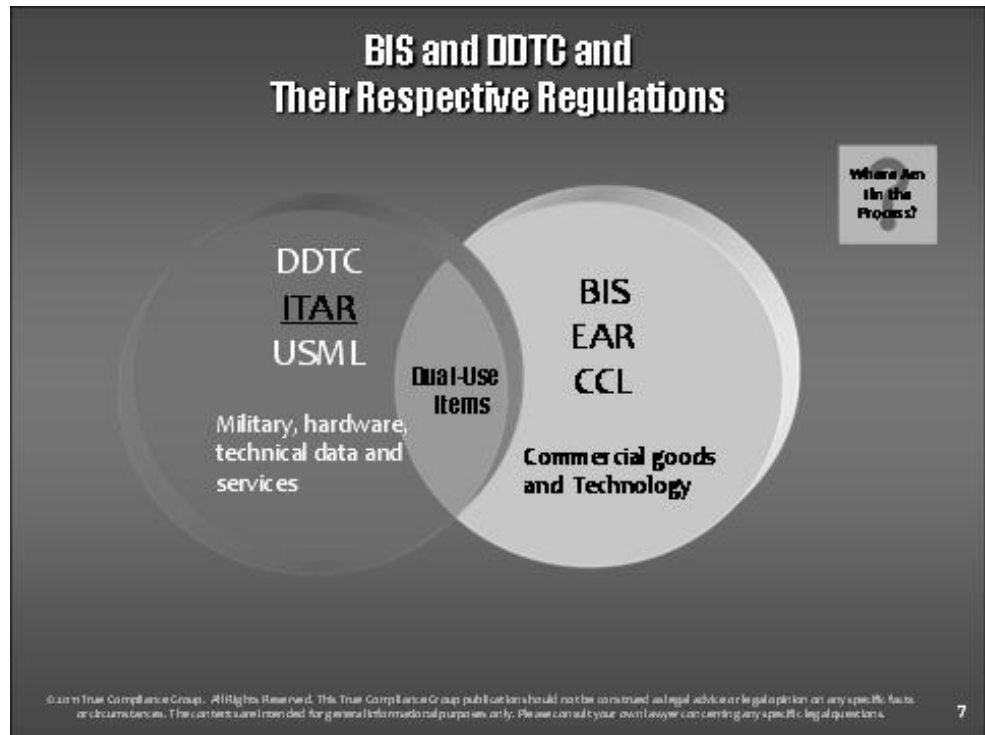
export control regime in an Export Control Reform Initiative that would also affect deemed export licensing and enforcement. Also, in August 2009, the President created an interagency task force to examine proposed export control reforms and in November 2010, signed an executive order establishing an Export Enforcement Coordination Center to coordinate and strengthen the U.S. government’s export enforcement efforts, including for deemed exports. *See* Executive Order 13558, 75 Fed. Reg. 69573 (Nov. 9, 2010).

<sup>2</sup> [www.bis.doc.gov/](http://www.bis.doc.gov/).

State's DDTC governs defense articles and services and technical data, including space and satellite articles.<sup>3</sup>

### What Are the Export Regulations?

DDTC's regulations are called International Traffic in Arms Regulations (ITAR). ITAR is located in 122 CFR Parts 120–130. Part 121 of ITAR is called the U.S. Munitions List (USML).<sup>4</sup> The USML is used to classify defense articles and services, technical data, and some dual-use items. BIS's regulations are called Export Administration Regulations (EAR.) EAR can be found in 15 CFR Parts 730 to 774. Part 774, Supp. 1, is the Commerce Control List (CCL).<sup>5</sup> The CCL is used to classify commercial items, technology, and some dual-use items.



<sup>3</sup> [www.pmdtc.state.gov/](http://www.pmdtc.state.gov/).

<sup>4</sup> [www.pmdtc.state.gov/regulations\\_laws/itar\\_official.html](http://www.pmdtc.state.gov/regulations_laws/itar_official.html).

<sup>5</sup> [www.gpo.gov/bis/ear/ear\\_data.html](http://www.gpo.gov/bis/ear/ear_data.html).

### Foreign Person Under ITAR or EAR

ITAR §120.16 defines “Foreign Person” as: “Any natural person who is not a lawful permanent resident as defined by 8 USC §1101(a)(20)<sup>6</sup> or who is not a protected individual as defined by 8 USC §1324b(a)(3).”<sup>7</sup> EAR §734.2(b)(2) and Part 772 uses the inverse of “Foreign Person,” focusing on “U.S. Persons,” defined as “[a]ny individual who is a citizen of the United States, a permanent resident alien of the United States, or a protected individual as defined by 8 USC §1324b(a)(3).”

Translated, “Foreign Person” means a person, who is not a U.S. citizen, a permanent resident, or a person granted status as a “protected individual” because of his or her citizenship (such as political refugees or asylum holders.) On a practical level, the concern is that the company will release controlled information to the Foreign Person. Such a release would be considered an “export” to the Foreign Person’s country of citizenship or birth. For the license determination attestation required in Part 6 of Form I-129, one must determine whether to use the BIS or DDTC’s standard of Foreign Person.

If you have Technology controlled by EAR, you will apply BIS’s standard. BIS is straightforward and looks to the most recent country of citizenship or nationality. For example, a Canadian citizen born in China will be considered a Canadian National under EAR. On the other hand, if you have Technical Data controlled by ITAR, you will apply DDTC’s standard. DDTC’s current policy is to look at the person’s country of birth *and* current citizenship and will defer to the most “sensitive” country. For example, a Canadian citizen born in China will be considered a Chinese national under ITAR.

So what are the chances of actually getting a license for a beneficiary? ITAR 126.1 has a “Prohibited Export List.”<sup>8</sup> EAR has its own version called the “Embargoed Countries List.”<sup>9</sup> Both list countries to which DDTC and EAR prohibit exports. This means, at the very least, you will need a license to export to these countries, or to a Foreign Person “from” these countries. Whether or not you are able to obtain a license

---

<sup>6</sup> “The term “lawfully admitted for permanent residence” means the status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws, such status not having changed.”

<sup>7</sup> (3) “Protected individual” defined: As used in paragraph (1), the term “protected individual” means an individual who—

(A) is a citizen or national of the United States, or

(B) is an alien who is lawfully admitted for permanent residence, is granted the status of an alien lawfully admitted for temporary residence under section 1160(a) or 1255a(a)(1) of this title, is admitted as a refugee under section 1157 of this title, or is granted asylum under section 1158 of this title; but does not include

(i) an alien who fails to apply for naturalization within six months of the date the alien first becomes eligible (by virtue of period of lawful permanent residence) to apply for naturalization or, if later, within six months after November 6, 1986, and

(ii) an alien who has applied on a timely basis, but has not been naturalized as a citizen within 2 years after the date of the application, unless the alien can establish that the alien is actively pursuing naturalization, except that time consumed in the Service’s processing the application shall not be counted toward the 2-year period.

<sup>8</sup> [www.pmdtc.state.gov/regulations\\_laws/documents/official\\_itar/ITAR\\_Part\\_126.pdf](http://www.pmdtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf).

<sup>9</sup> [www.bis.doc.gov/pdf/jp8embar.pdf](http://www.bis.doc.gov/pdf/jp8embar.pdf).

will depend on the Technology or Technical Data and the country. So for example, a company might have an extremely difficult time, if they are able at all, to obtain a license for a Chinese foreign national from the DDTC.

### **Technology or Technical Data**

“Technology”—the DDTC/ITAR term—and “Technical Data”—the BIS/EAR term—are very similar concepts. Part 772 of EAR defines “Technology” as specific information necessary for the development, production, or use of a product. This includes, in general, blueprints, drawings, photographs, plans, instructions and documentation related to commercial and some dual-use items.

“Technical Data” under ITAR §120.10 is information required for the design, development, production, manufacture, assembly, operation, repair testing, maintenance, or modification of defense articles. This includes, in general, blueprints, drawings, photographs, plans, instructions, and documentation related to a defense and some dual-use articles and services.

Sometimes it easier to define Technical Data or Technology by what they are not. According to ITAR section 120.10(a)(5), technical data are not:

- Information in the public domain;
- Information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities; or
- Basic marketing information on function or purpose or general system descriptions of defense articles.

As per Part 734 of EAR, “technology” is not subject to BIS’s control if it is:

- Already published or will be published;
- Arising during or resulting from fundamental research;
- Educational; or
- Included in certain patent applications.

The first exclusion is the public domain. If technology or technical data is in the public domain, it is generally not controlled. Public domain means that the information is available:

- At libraries;
- Through patents;
- Publically disseminated at trade shows and conferences;
- At newsstands, bookstores and through subscriptions; or is
- Non-proprietary fundamental research.

It is important to note, just because something is on the Internet or published does not mean it *should* be; something that appears on the Internet is not necessarily in the public domain. Under EAR, posting on the Internet or other publication is sufficient for the technology to be deemed in the public domain. Under the ITAR, the publication must be authorized.

In addition, technology or technical data is generally not controlled if it is considered to be general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities. Along the same lines, “fundamental research” is also excluded from the definition.

### **Fundamental Research vs. Proprietary Research**

“Fundamental research” is basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community. It is distinguished from proprietary research and from industrial development, design, production, and product utilizations, the results of which ordinarily are restricted for proprietary and/or specific national security reasons. Normally, the results of fundamental research are published in scientific literature, thus making it publicly available. Research that is intended for publication, whether it is ever accepted by a scientific journal or not, is considered to be “fundamental research.” A large segment of academic research is considered “fundamental research.”

In certain situations, a university may have several departments that are conducting research under contract with private corporations. Some of this research is referred to as controlled “development” technology. Many researchers, including visiting faculty, post-graduate fellows, and research assistants are foreign nationals working on controlled “development” technology research. In these situations, one must look at the research and the contract terms for release of the results of the research. If there are no conditions placed on the research, and it is the intent of the research team to publish its findings in scientific literature, then it is considered “fundamental research,” and would be not be controlled.

If the contract requires that the private corporation review the findings of the research team with the intent of controlling what results are to be released in open literature, then the research is considered proprietary, and would be Technology or Technical Data. This analysis examining whether it is “fundamental research” or “proprietary research” also applies to situations where universities conduct research under U.S. government sponsorship. However, some government contracts may subject the university to separate restrictions on dissemination such as security classification.

### **E, F and J Nonimmigrants May Also Be Subject to Export Laws**

While the certification in Part 6 is for foreign nationals under the H-1B, H-1B1, L-1, or O-1A visa, foreign nationals employed under E, F, and J nonimmigrant visa classification are considered foreign persons under ITAR and EAR and may require a license as well. You must be cognitive of subsequent applications filed by graduating students or post-doctoral researchers entering private industry. Although a U.S. university would not need a license to allow a Chinese graduate student to engage in technological research if the results of that research are to be published in a professional journal, a U.S. firm that hired the same Chinese national to engage in proprietary research to develop a new commercial product may have to secure a license. Thus, when that Chinese individual files a change-of-status application to another nonimmigrant classification, an export license may be required.

**Release: Export and Deemed Export**

Generally speaking, an export is a shipment or transmission of items or technology from the United States to a foreign country. But it is not limited to those situations. Export also includes the release of technology outside the United States as well as the release of technology inside the United States knowing that it will be exported outside the United States, *i.e.*, re-exported.

A “Deemed Export” is the release of technology, information, or software to a foreign person. An export to a foreign person is deemed to be an export to the person’s country of origin.

A “release” or Deemed Export can occur in many ways, including:

- Visual inspection/tours of equipment and facilities (even with vendors, janitors, and consultants);
- Verbal exchanges of technology (including marketing meetings, staff meetings, and casual conversations);
- E-mails, faxes, text messages, and posting on the Internet;
- Access to network or database containing technology or technical data.

If you have technology controlled by EAR (commercial and dual-use), you will apply BIS’s standard. (BIS looks to the most recent country of citizenship or nationality.) On the other hand, if you have Technical Data controlled by ITAR (defense article and services), you will apply DDTC’s standard. (DDTC’s current policy is to look at the person’s country of birth and current citizenship.)

Releasing Technical Data or Technology to someone who is *not* a Foreign Person is just a release. There is no issue, if, for example, a U.S. citizen provides unclassified specs for a military component (Technical Data) to another U.S. citizen. Releasing technical data or technology that is *not* controlled to a Foreign Person similarly is just a release. For example, a U.S. citizen may provide a Chinese foreign national with the blueprints to make a ballpoint pen (not controlled technology). The concern is when Technical Data or Technology is released to a Foreign Person. This release is known as a “Deemed Export.” It does not matter if the release occurs in the United States or abroad.

**Preventing Access of Controlled Data in the Workplace/Firewalls**

In reality, computer networks and electronics exist in every business workplace, providing countless opportunities for deemed export violations to occur. Any foreign person, including technical and information technology (IT) support personnel, may require export licenses if they have unrestricted access to controlled data. Employers with foreign employees that have any amount of controlled Technical Data on their computer systems (or even printers or smart phones, etc.) must devise a system to separate controlled from uncontrolled Technology or Technical Data. Your clients should consider security options such as password protection for individual documents, protected databases, and secure subnets as well as a designated compliance specialist who is responsible for firewalling such Technology or Technical Data from foreign employees, contractors, or even visitors.

### **Does the Company Have Foreign National Computer Support Personnel with “Master Access?”**

Many companies grant “master” access to IT support staff over computer systems containing controlled technical data to enable them to maintain and troubleshoot systems, implement access controls, and conduct backup and recovery functions. Export control regulations apply to every employee, including those in the technical field and those who provide support functions. The issue is not whether an individual accessed the controlled technology, but whether the individual simply *had access*. Merely having access to the entire system creates the possibility that the IT support personnel could visually inspect the data and thus subject the company to a “deemed export” violation. This issue is further complicated when companies outsource IT support, creating additional risks of export violations.

### **Do You Need a License for Your Beneficiary?**

For purposes of completing Part 6 of the Form I-129, the Petitioner is required to make a determination if an export license from either the DDTC or BIS is required for the Beneficiary to receive technology or technical data from the company. A license determination to export Technology or Technical Data *to a Foreign Person* (as distinguished from an exporting an item/service to a foreign country) is a three tiered-process involving Classification, License Determination, and Restricted Party Screen.

#### ***1. Classification***

Classification can be a subjective, difficult process with lots of grey area, but in general there are three ways to classify:

- Get it in writing from the manufacturer;
- Self-classify;
- Request a Commodity Jurisdiction (CJ) from the DDTC or Commodity Classification from BIS.

Classifying the item, information, or service using either ITAR or EAR, and specifically, the USML or CCL, will depend on whether BIS or DDTC has jurisdiction. Everything has a classification, but keep in mind, it is either under ITAR or EAR, not both.

In effect, your client will need to look at all their operations and evaluate whether they work with ITAR or EAR controlled items or data *at all*. Essentially, they are going to classify their operations as a whole and then drill down to individual divisions and projects. Keep in mind, this is a very complex process that takes into account many different factors and usually requires experience/expert advice.

#### ***2. License Determination***

Once the information is classified, it will be either ITAR or have an ECCN (Export Control Classification Number) under EAR. The ECCN is a five-digit number that will look, for example, like this: “9A991.” At the end of every section of the CCL is EAR99. Items subject to the EAR that are not elsewhere specified (N.E.S.) in this CCL category or in any other category in the CCL are designated as EAR99. This designation usually

ships without a license unless it is to an embargoed country. If it's ITAR, you will need a license 99 percent of the time, unless there is an exemption. With EAR, there are three ways to export something: (1) With a license (2) with exemption or (3) no license required (NLR) For the purposes of Part 6, if it is not ITAR, one must look at the ECCN and the BIS standard for Foreign Person (most recent country of citizenship or nationality) and assuming no exemption applies, cross-reference the ECCN Controls against the Commerce Country Chart. Keep in mind, this is a very complex process that takes into account many different factors and usually requires experience/expert advice.

### 3. *Restricted Party Screen*

This requires a check of the names of all parties to the transaction (Foreign Person, customer, vendor, freight forwarder, etc.) against a list of individuals and organizations that are prohibited from receiving U.S. exports *at all*, or requires a license even for uncontrolled items and data. If you will be exporting *anything*, even if it is EAR99 and you *do not* need a license, you still need to do a Restricted Party Screen for all Parties to the transaction.<sup>10</sup> These lists include but are not limited to:

- Denied Persons List
- Entities List
- Unverified List
- Specially Designated Nationals and Blocked Persons List
- State Debarment List
- Non-Proliferation Sanctions
- General Orders under Part 736

#### **Use of Subcontractors**

What if a company hires subcontractors, or possibly foreign nationals in another country, to develop or produce a controlled item? This is often referred to as a “deemed re-export” situation, where there is a transfer of controlled U.S. technology to a third-country national overseas. For example, a U.S. company needs to transfer its controlled proprietary technology to a company in the United Kingdom. The UK firm employs an individual from India who is not a permanent resident of the United Kingdom, or of the United States, and who will need the controlled proprietary technology to perform his or her assigned duties. The U.S. company must obtain an export license, as required, for the Indian national or the UK company or both.

#### **How Long Does It Take to Obtain a License and How Long Are They Valid?**

Prior to applying for a license from BIS or DDTC, a company must first register. BIS processes deemed export licenses for Foreign Persons using its SNAP-R system. The process can take a month or significantly more time, depending on the company, the technology, and the person's nationality and background. The license is valid for two

---

<sup>10</sup> [www.export.gov/ecr/eg\\_main\\_023148.asp](http://www.export.gov/ecr/eg_main_023148.asp).

years. However, since an H-1B work visa is typically valid for 36 months, a license applicant may note in its application the expiration date of a visa that is beyond the standard two-year validity period of a license, and request a matching, extended, validity period, in accordance with section 748.6(g) of the EAR. The DDTC takes approximately two to four weeks to process export license applications for Foreign Persons (DSP5) through its D-Trade system. Again, this can vary by company and person. This license is generally valid for four years.

### ***What Happens if an Export License Application Is Denied?***

There is no right to judicial review if a license application is denied. Both the DDTC and BIS can conduct an administrative review, but rarely overturn the decisions of its own agency.

### ***What Happens After an Export License Is Issued?***

BIS and DDTC issue licenses that are usually subject to restrictions that are set forth in the license itself. BIS refers to these restrictions as “riders and conditions,” while the DDTC refers to them as “limitations and provisos.” These restrictions can be burdensome, and in some cases, the employee is essentially prohibited from performing the job for which he or she was hired. Licenses issued by the BIS increasingly contain the use of “standard” restrictions that have nothing to do with the intended technology transfer. Standard restrictions include the following items:

- No access to the ITAR technical data or classified information
- Maintain records of green cards issued to foreign nationals
- New application if new access to controlled technology
- Use of encryption products, but not technology permitted
- Must inform foreign nationals of all license conditions
- Must establish procedures to ensure compliance with license conditions, monitored by Commerce Department

### ***When Is a Compliance Program Needed?***

In addition to various other types of organizations, if your client is a U.S. manufacturer, exporter, or university, it should have an export compliance program, regardless of whether they have foreign nationals or not. Export compliance touches every area of operations, whether it is human resources, legal, research and development, marketing, sales, or shipping/receiving. An export compliance program can do much more than simply fulfill the minimal obligations set forth by the DDTC or BIS (or other government agencies.) An effective compliance program will not only help prevent violations, but is a mandatory mitigating factor should violations occur. At a minimum, an export compliance program should address the following:

- Organization structure
- Corporate commitment and policy
- Identification, receipt and tracking of ITAR/EAR controlled items/technical data and technology

- Restricted/prohibited exports and transfers
- Recordkeeping
- Internal monitoring
- Training
- Violations and penalties

On a practical level, every department should have integrated export compliance procedures. For example, the HR department may require that new hires fill out comprehensive questionnaires detailing biographic information, employment history, educational history, and professional affiliations. They may want to require background screening procedures (ensuring that such procedures are nondiscriminatory.) For Foreign Persons, HR may also want to use an interdepartmental checklist to ensure that all departments and relevant persons (including the various department heads, immigration counsel, and export advisors) are aware of and have met export requirements for that prospective employee.

### **Penalties for Violations**

Your client may be reluctant to spend any time or money on a compliance program or training. We suggest that they need only look to the penalties for violations for some incentive. In addition to the fines and penalties for perjury, ITAR penalties include, but are not limited to:

- Up to \$1 million fine per criminal violation, or imprisonment of up to 10 years *or* both;
- Up to \$500,000 fine per civil violation (note: there can be multiple violations), and possibly also:
  - Seizure and forfeiture of goods;
  - Prohibited from engaging export activity;
  - Interim suspension with direct or indirect prohibition of exporting goods;
  - Debarment from federal government contracts.
- Penalties for violating EAR include, but are not limited to:
  - Up to 20 years imprisonment and \$1 million per criminal violation;
  - Up to \$250,000 per civil violation or twice the value of the export (whichever is greater);
  - Prohibition from engaging in export activity.

### **Expect Delays at Consular Posts: The Technology Alert List and Visas Mantis Security Advisory Opinions**

The practice of immigration law now requires a thorough analysis of not only an alien's entire employment and immigration history, but also a company's background and business. Getting the petitioner to address the export control issue, filing and getting your visa approved are just part of the visa application process. If the beneficiary is abroad and waiting to enter the United States or travels for business or vacation, expect delays at

consular posts abroad. Now that consular officers have easy access to PIMS and often request copies of the I-129, which now includes the export licensing question, many visa applicants engaged in science, engineering and technology (even if an export license is not required) are likely to experience delays in visa issuance based on the initiation of a Visas Mantis security advisory opinion (SAO).

The Visas Mantis program is an SAO procedure designed to ensure that sensitive technology is not stolen or inappropriately shared with those who would use it to harm the United States and its allies. In assessing these threats, DOS relies primarily on the Technology Alert List (TAL)<sup>11</sup> to make its determinations. The TAL is also designed to specifically provide guidance for use in cases that may fall under the purview of Immigration and Nationality Act (INA) §212(a)(3)(A), which renders aliens inadmissible where there is reason to believe they are seeking to enter the United States to violate or evade U.S. laws prohibiting the export of goods, technology, or sensitive information from the United States. Updated in 2002, the TAL was designed to assist in the effort to prevent the transfer of sensitive technology or material (*e.g.*, controlled nuclear or biotechnical information) from falling into the wrong hands and being used by hostile individuals. The increasing sophistication of off-the-shelf technology, dual-use technologies (technologies that have both civilian and military applications), allegations of lack of sufficient information about and controls on foreign students in the United States, tensions in the Middle East, and the 9/11 terrorist attacks combined to renew concern among the law enforcement and intelligence communities that controlled U.S.-origin goods and information are vulnerable.

The 2002 revised TAL consisted of two parts: a Critical Fields List (CFL)<sup>12</sup> of major fields of technology transfer concern, including those subject to export controls for

---

<sup>11</sup> The TAL was originally designed to help maintain technological superiority over the Warsaw Pact and was targeted at individuals from the Soviet Union and other Communist countries. In 1996, the TAL was revised to broaden its focus and reflect more accurately current laws restricting or prohibiting the export of goods and technologies. These laws are designed to further four important security objectives: (i) Stem the proliferation of weapons of mass destruction and missile delivery systems; (ii) Restrain the development of destabilizing conventional military capabilities in certain regions of the world; (iii) Prevent the transfer of arms and sensitive dual-use items to terrorist states; and (iv) Maintain U.S. advantages in certain militarily critical technologies.

<sup>12</sup> The critical fields list, which constitutes the Technology Alert List (TAL), is as follows: (A) Conventional Munitions—technologies associated with warhead and large caliber projectiles, reactive armor and warhead defeat systems, fusing, and arming systems, electronic countermeasures and systems, new or novel explosives and formulations, automated explosive detection methods and equipment; (B) Nuclear Technology—technologies associated with the production and use of nuclear material for both peaceful and military applications, including enrichment of fissile material, reprocessing irradiated nuclear fuel to recover produced plutonium, production of heavy water for moderator material, plutonium and tritium handling. Also, certain associated technologies related to nuclear physics and/or nuclear engineering, including materials, equipment or technology associated with power reactors, breeder and production reactors, fissile or special nuclear materials, uranium enrichment, including gaseous diffusion, centrifuge, aerodynamic, chemical, Electromagnetic Isotopic Separation, Laser Isotope Separation, spent fuel reprocessing, plutonium, mixed oxide nuclear research Inertial Confinement Fusion, magnetic confinement fusion, laser fusion, high power lasers, plasma, nuclear fuel fabrication including Mixed Oxide (uranium-plutonium) fuels, heavy water production, tritium production and use, hardening technology; (C) Rocket Systems—(including ballistic missile systems, space launch vehicles and sounding rockets) and Unmanned Air Vehicles (UAV)

*Cont'd*

(including cruise missiles, target drones, and reconnaissance drones)—technologies associated with rocket systems and UAV systems (the technology needed to develop a satellite launch vehicle is virtually identical to that needed to build a ballistic missile); (D) Rocket System and Unmanned Air Vehicle Subsystems—Propulsion technologies include solid rocket motor stages, and liquid propellant engines. Other critical subsystems include re-entry vehicles, guidance sets, thrust vector controls and warhead safing, arming and fusing. Many of these technologies are dual-use and include liquid and solid rocket propulsion systems, missile propulsion and systems integration, individual rocket stages or staging/separation mechanism, aerospace thermal (such as super alloys) and high-performance structures, propulsion systems test facilities. (E) Navigation, Avionics and Flight Control Useable in Rocket Systems and UAV—These capabilities directly determine the delivery accuracy and lethality of both unguided and guided weapons. The long-term costs to design, build and apply these technologies have been a limiting proliferation factor. Technologies include those associated with internal navigation systems, tracking and terminal homing devices, accelerometers and gyroscopes, rocket and UAV and flight control systems and global positioning system; (F) Chemical, Biotechnology and Biomedical Engineering—technology used to produce chemical and biological weapons is inherently dual-use. The same technologies that could be applied to develop and produce chemical and biological weapons are used widely by civilian research laboratories and industry; these technologies are relatively common in many countries. Advanced biotechnology has the potential to support biological weapons research. In the biological area, areas of interest in technologies associated with Aerobiology (study of microorganisms found in the air or in aerosol form), Biochemistry, Pharmacology, Immunology Virology Bacteriology, Mycology, Microbiology, Growth and culturing of microorganisms, Pathology (study of diseases), Toxicology, Study of toxins, Virulence factors, Genetic engineering, recombinant DNA technology, Identification of nucleic acid sequences associated with pathogenicity, Freeze-drying (lyophilization), Fermentation technology, Cross-filtration equipment, High “DOP-rated filters” (e.g., HEPA filters, ULPA filters), Microencapsulation, Aerosol sprayers and technology, aerosol and aerosolization technology, Spray or drum drying technology, Milling equipment or technology intended for the production of micron-sized particles, Technology for eliminating electrostatic charges of small particles, Flight training, Crop-dusting, aerosol dissemination, Unmanned aerial vehicle technology, Fuses, detonators, and other munitions technology, Submunitions technology, Computer modeling of dissemination or contagion, Chemical absorption (nuclear-biological-chemical protection). In the chemical area, includes Organo-phosphate chemistry, Neurochemistry, Chemical engineering, Chemical separation technology, Pesticide production technology, Pharmaceutical production technology, Chemical separation technology, Toxicology, Pharmacology, Neurology, Immunology, Detection of toxic chemical aerosols, Chemical absorption (Nuclear-Biological-Chemical protection), Production of glass-lined steel reactors/vessels, pipes, flanges, and other equipment, Aerosol sprayers and technology, Flight training, Crop-dusting, aerosol dissemination, Unmanned Aerial Vehicle technology, Fuses, detonators, and other munitions technology, Submunitions technology, Computer modeling of dissemination; (G) Remote Sensing, Imaging and Reconnaissance—satellite and aircraft remote sensing technologies are inherently dual-use; increasingly sophisticated technologies can be used for civilian imagery projects or for military and intelligence reconnaissance activities. Drones and remotely piloted vehicles also augment satellite capabilities. Key-word associated technologies include, Remote sensing satellites, High resolution multi-spectral, electro-optical and radar data/imagery, Imagery instruments, cameras, optics, and synthetic aperture radar systems, Ground receiving stations and data/image processing systems, Photogrammetry, Imagery data and information products, Piloted aircraft, UAV, Remotely-piloted vehicles; and drones; (H) Advanced Computer/Microelectronic Technology—advanced computers and software play a useful (but not necessarily critical) role in the development and deployment of missiles and missile systems, and in the development and production of nuclear weapons. Advanced computer capabilities are also used in over-the-horizon targeting airborne early warning targeting, Electronic Countermeasures (ECM) processors. These technologies are associated with Supercomputing, hybrid computing, Speech processing/recognition systems, Neural networks, Data fusion, Quantum wells, resonant tunneling, Superconductivity, Advance optoelectronics, Acoustic wave devices, Superconducting electron devices, Flash discharge type x-ray systems, Frequency synthesizers, Microcomputer compensated crystal oscillators; (I) Materials Technology—the metallic, ceramic and composite materials are primarily related to structural functions in aircraft, spacecraft, missiles, undersea vehicles, and propulsion devices. Polymers provide seals and sealants for containment of identified fluids and lubricants for various vehicles and devices. High density graphite is used in missile nosetips, jet

*Cont'd*

nonproliferation reasons, and DOS's list of designated State Sponsors of Terrorism, also known as the "T-4" countries.<sup>13</sup> Although restrictions on the export of controlled goods and technologies applies to scientific and technical visitors from all countries, DOS instructs posts that applicants from countries designated as "state sponsors of terrorism" seeking to engage in one of the critical fields warrant special scrutiny and mandatory security advisory opinion (SAO) checks.<sup>14</sup> The TAL is no longer publicly available and has been removed from the DOS website.<sup>15</sup> However, DOS confirms that it reviews the

---

vanes and nozzle throats. Selected specialty materials (*i.e.*, stealth and the performance of these materials) provide critical capabilities that exploit electromagnetic absorption, magnetic, or superconductivity characteristics. These technologies are associated with advanced metals and alloys, Non-composite ceramic materials, Ceramic, cermet, organic and carbon materials, Polymeric materials, Synthetics fluids, Hot isostatic, Densifications, Intermetallic, Organometals, Liquid and solid lubricant, Magnetic metals and superconductive conductors; (J) Information Security—Technologies associated with cryptography and cryptographic systems to ensure secrecy for communications, video, data and related software; (K) Laser and Directed Energy Systems Technology—Lasers have critical military applications, including incorporation in guided ordinance such as laser guided bombs and ranging devices. Directed energy technologies are used to generate electromagnetic radiation or particle beams and to project that energy on a specific target. Kinetic energy technologies are those used to impart a high velocity to a mass and direct it to a target. Directed energy and kinetic energy technologies have potential utility in countering missiles and other applications. Look for technologies associated with Atomic Vapor Laser Isotope Separation, Molecular Laser Isotope Separation, High Energy Lasers (*i.e.*, laser welders), Low Energy Lasers, Semiconductor lasers, Free electron lasers, Directed Energy systems, Kinetic Energy systems, Particle beam, beam rider, electromagnetic guns, Optoelectronics/electro-optics (Europe), Optical tracking (*i.e.*, target designators), High energy density, High-speed pulse generation, pulsed power, Hypersonic and/or hypervelocity, Magnetohydrodynamics; (L) Sensors and Sensor Technology—Sensors provide real-time information and data, and could provide a significant military advantage in a conflict. Marine acoustics is critical in anti-submarine warfare; gravity meters are essential for missile launch calibration. Includes technologies associated with Marine acoustics, Optical sensors, Night vision devices, image intensification devices, Gravity meters, High speed photographic equipment, Magnetometers; (M) Marine Technology—Marine technologies are often associated with submarines and other deep submersible vessels; propulsion systems designed for undersea use and navigation and quieting systems are associated with reducing detectability and enhancing operations survivability. Includes technologies connected with Submarines and submersibles, Undersea robots, Marine propulsion systems, Signature recognition, Acoustic and non-acoustic detection, Acoustic, wake, radar and magnetic signature reduction, Magnetohydrodynamics, Stirling engines and other air independent propulsion systems; (N) Robotics—Technologies associated with Artificial intelligence, Automation, Computer-controlled machine tools, Pattern recognition technologies; and (O) Urban Planning—Expertise in construction or design of systems or technologies necessary to sustain modern urban societies. (*Please note:* Urban Planning may not fall under the purview of INA §212(a)(3)(A), U.S. technology transfer laws, or any other U.S. law or regulation. However, Urban Planning is a special interest item and posts are requested to refer such visa application requests to CA/VO/L/C for further review.) Technologies/skills include Architecture, Civil engineering, Community development, Environmental planning, Geography, Housing, Landscape architecture, Land use and comprehensive planning, and Urban design. *See* "State Dept. Updates Guidance on Technology Alert Checks," *posted on* AILA InfoNet at Doc. No. 03030449 (*posted* Mar. 4, 2003).

<sup>13</sup> The current designated list of state sponsors of terrorism includes Cuba, Iran, Sudan and Syria.

<sup>14</sup> *See* State Department Cable, "State Dept. Updates Guidance of Technology Alert Checks *posted on* AILA InfoNet at Doc. No. 03030449 (*posted* Mar. 4, 2003).

<sup>15</sup> Anecdotal reports indicate that the TAL was removed from the DOS website because of concerns that applicants used the TAL to "tailor" their CVs before interviews at posts in an attempt to avoid initiation of a Mantis SAO. When asked about the removal of the TAL from the website based on concerns that there is no current guidance on what technologies may be on the list, DOS stated that the TAL is "not produced to assist

*Cont'd*

TAL each year, eliminating items that do not appear to pose a risk and adding any new areas of concern.<sup>16</sup>

### ***Documents an Applicant with Potential Mantis Issues Should Bring to an Interview***

Anecdotal reports confirm that many visa applicants involved not only in research, but also in high-tech industries, are routinely subject to Visas Mantis SAOs (usually referred to as “administrative processing under 221(g)”). Practitioners also report that these checks have become routine at certain consular posts, particularly in China and India.

Applicants involved in any activities that have potential “dual use” applications should bring the following documents to an interview:

- Complete résumé (and if accompanying the applicant, a professional spouse’s résumé);
- Complete list of publications of the applicant (and spouse’s publications);
- List of references in the applicant’s country of birth or residence;
- Detailed descriptions of the applicant’s proposed research or work in the United States, explaining the nature of the work, specific job duties, and project descriptions, and if possible, details distinguishing how the work has no possible military applications;
- Documentation to show that the information is in the public domain;
- Documentation to show that the information is found in academic courses (where applicable);
- Documentation to show that export control compliance counsel or the appropriate export control compliance officer at your organization has determined that an export license is not required;
- If a company has an export license, it is sometimes helpful to bring a copy of the license as well. However, the existence of an export license does not eliminate or replace the need for a Mantis SAO if necessary.<sup>17</sup>

---

business in making plans. Making available to the public a detailed list of sensitive technologies would be invaluable to those seeking to avoid undue scrutiny of technology transfer activities.” See “DOS Answers AILA Questions,” (Oct. 2004), *published on AILA InfoNet at Doc. No. 04120760 (posted Dec. 7, 2004)*.

<sup>16</sup> See Testimony of Deputy Assistant Secretary of State for Visa Services S. A. “Tony” Edson, before the U.S. House of Representatives, Committee on Science and Technology Subcommittee on Research and Science Education, House Committee on Science and Technology, Feb. 7, 2008 *available at [http://travel.state.gov/law/legal/testimony/testimony\\_3950.html](http://travel.state.gov/law/legal/testimony/testimony_3950.html)*.

<sup>17</sup> The provisions at 9 *Foreign Affairs Manual* (FAM) 40.31 N5.1-1(2) state that “if an applicant for a visa plans to export equipment or information on [the TAL] from the United States to any country without proof that a competent U.S. governmental authority has already approved an export license, the post should suspend processing, deny the application under §221(g) and submit a SAO to the department.” According to DOS, the existence of such a license does not mean that an applicant is not subject to TAL and not subject to an SAO. It is still possible that the applicant, himself, is of concern on national security grounds. See “DOS Answers AILA Questions,” (Oct. 2004), *published on AILA InfoNet at Doc. No. 04120760 (posted Dec. 7, 2004)*.

It also appears that many nonimmigrant visa applicants who are subjected to a Mantis security check are considered “persons of interest” when they arrive in the United States. There have been numerous anecdotal reports that the FBI has made follow-up visits to universities, as well as to private companies, to check up on such individuals to ensure that they are in full compliance with the terms of their nonimmigrant status.

### *Validity of Visas Mantis Clearances*

The maximum validity of the Visas Mantis clearances for F-1, J-1, H-1B, L-1, O-1, and B-1/B-2 visas was extended in 2005,<sup>18</sup> allowing applicants to reapply for visas without undergoing frequent Mantis checks, if returning to the previous program of study or professional assignment. However, consular officers have discretion, if warranted, to initiate a Mantis SAO.

The validity period for F-1 applicants is up to the length of the academic program, to a maximum of four years. However, if the student changes programs, the clearance is no longer valid and a SAO will be initiated if the applicant applies for a new visa. H-1B, J-1, and L-1 applicants are eligible for clearances valid for the duration of their approved activity to a maximum of two years. If the nature of the foreign national’s activities change, the clearance ceases to be valid and a new SAO is required.

B-1/B-2 applicants can receive a Mantis clearance valid for one year, provided that that the original purpose for travel, as stated in the visa application has not changed on subsequent trips.

Keep in mind, the new clearance validity periods do not apply to applicants from state sponsors of terrorism and these extended validities apply to any applicants who are re-applying for a visa within 12 months of the previously issued visa.

The Department of State reports that most Visas Mantis SAOs are cleared within 60 days. However, if a Mantis security check has been pending for more than 60 days, one may call the Visa Office public inquiries number at (202) 663-1225 [or fax at (202) 663-3899 or send an e-mail inquiry to [legalnet@state.gov](mailto:legalnet@state.gov)].

The increasing sophistication of technology has completely changed the world in which we live. An export is no longer just a shipment of physical goods, but now includes all sorts of technologies and services. At the same time, the number of foreign nationals in the U.S. workforce will continue to rise as statistics reflect an increasing number of foreign graduate students, post-doctoral fellows, and researchers in the United States, combined with a decline in the number of U.S. graduates in the scientific, engineering, and high-tech fields. As government agencies continue to monitor the activities of foreign nationals by implementing increasingly sophisticated security measures to address national security concerns, enforcement to abate the unlawful transfer of sensitive technologies will undoubtedly increase. In recent years, companies have experienced an increase in monitoring and requests for information on all types of nonimmigrant visa applications, inquiries about particular projects on which the

---

<sup>18</sup> See “Some Visas Mantis Clearances Extended,” published on AILA InfoNet at Doc. No. 05021460 (posted Feb. 14, 2005).

individuals are working, Fraud Detection and National Security unannounced worksite visits, including interviews with employers, licensing checks, and an increase in audits by a host of government agencies including the BIS, DHS, Customs and Border Protection, Immigration and Customs Enforcement, and the FBI, to name a few. These developments signal a shift in government priorities and immigration practitioners can be sure that these issues will affect their clients.