COMPLIANCE WITH U.S. EXPORT AND REEXPORT CONTROLS

November 2013

By Benjamin H. Flowe, Jr.
Berliner, Corcoran & Rowe, L.L.P.
1101 17th Street, N.W., Suite 1100
Washington DC 20036

Phone: 202-293-5555
Fax: 202-293-9035
bflowe@bcr-dc.com

Compliance with U.S. Export and Reexport Controls

Benjamin H. Flowe, Jr.
November 2013

 bflowe@bcr-dc.com

 bflowe@bcr-dc.com

 bflowe@bcr-dc.com

 bflowe@bcr-dc.com

 bflowe@bcr-dc.com

 bflowe@bcr-dc.com

Attachments:
Customer Export Compliance Checklist Reference Form
Know Your Customer Guidelines
Country Groups from EAR Part 740

-#-

 bflowe@bcr-dc.com

BENJAMIN H. FLOWE, JR.
Attorney at Law
BERLINER, CORCORAN & ROWE, L.L.P.
1101 17th Street, N.W., Suite 1100
Washington DC 20036-4798

(202) 293-5555 **Telefax (202) 293-9035**

November 2013

Compliance with U.S. Export and Reexport Controls

1. Introduction

U.S. export control laws present a number of challenges. By their very nature, export controls are impediments to business. Even determining which U.S. agency regulates a particular export can be difficult. Despite how complex these laws can be, especially when applied to non-U.S. activities, U.S. government agencies expect foreign firms to know U.S. export control laws and to know their customers' businesses. To avoid potentially severe penalties, companies working with U.S. origin products and technologies should familiarize themselves with U.S. export control laws. Developing a systematic program to comply with export controls efficiently is also useful to reduce the burdens they impose on business.

Whenever certain controls are liberalized, as with the removal of many items from the U.S. Munitions List that is currently underway as part of the Obama Administration's Export Reform Initiative, there it a natural tendency to relax company compliance programs. This makes export compliance programs more important than ever. Liberalizations of traditional controls that were based on the technical sophistication of products, coupled with nonproliferation controls that are based on particular end-users and end-uses of less sophisticated products, have actually made controls more complex. Moreover, they shift most export compliance burdens from government licensing officers to company compliance personnel. The added freedom comes with added risks born by companies.

This paper is a summary of the law, but not a replacement for reviewing the laws themselves. Because this paper cannot possibly address all types of transactions, readers are encouraged to consult their attorneys, applicable U.S. government agencies, and knowledgeable consultants to address application of the law to specific facts.

2. Extraterritorial Application of U.S. Law.

Many companies get into trouble by assuming that their non-U.S. operations are not subject to U.S. laws. Unfortunately, the United States does assert jurisdiction over activities that occur wholly beyond U.S. borders, i.e., extraterritorially. Besides the export control laws of the territory in which they operate, companies are best advised to pay attention to U.S. reexport controls, like it or not.

U.S. export control laws and regulations apply extraterritorially to shipments made from outside the United States (referred to as "reexports") of: (a) U.S.-origin products, (b) foreign-made products that incorporate U.S.-origin components, and (c) foreign-made products that are the direct products of U.S.-origin technology. Most export control laws thus are based on the U.S. nexus to the items or technology being reexported and are not dependent on any personal

 bflowe@bcr-dc.com

connection of the exporter to the United States.[1] The United States asserts jurisdictional claims in part based on Destination Control Statements that must appear on U.S. export documentation, letters of assurance that are required to allow exports of modern technology under License Exception TSR, supporting documents for export licenses signed by the recipient, and other means of constructive notice to non-U.S. companies of U.S. jurisdiction.

Most major U.S. trading partners, particularly Germany, the United Kingdom, and most other EU countries, view the extraterritorial application of these U.S. laws as illegal under international law and their own laws. Nonetheless, the United States commonly imposes civil and criminal penalties on wholly foreign companies for violating U.S. export and reexport controls. Even if U.S. prosecutors cannot obtain personal jurisdiction over a company or an individual against which to assess fines or prison terms, it can publish the famous **Denial Orders** in the *Federal Register*, putting all U.S. exporters and reexporters of U.S. products on notice not to do business with the company that violated U.S. reexport control laws. That is a very powerful and effective sanction.

The United States has mostly enforced multilateral controls agreed to by other countries. Objecting to the United States when one is imposing the same types of export controls is difficult for other governments, as then notorious sanctions on Toshiba and Kongsberg in 1988 made clear. In contrast, the United States generally has not insisted on extraterritorial enforcement of unilateral U.S. controls in significant cases, placing greater importance on the foreign relations interests of allied governments. Thus, the major disagreement over proper application of international law, and the territorial or extraterritorial theory of jurisdiction, has been largely left unresolved in favor of an uneasy but more pragmatic solution. In practice, except for the rare instances in which other countries challenge U.S. export controls or sanctions (e.g., European challenges to the U.S. Helms-Burton law on Cuba, the Iran-Libya Sanctions Act of 1996, and the Siberian Pipeline sanctions of the early 1980s), the United States and most allies reluctantly agree to disagree and work out individual cases as appropriate under the circumstances. On occasion, an EU Member Government will fight vigorously on principle for an individual company facing U.S. sanctions and use political or other leverage to persuade U.S. prosecutors to settle a case against its national on more reasonable terms than the prosecutors otherwise would prefer. More often, the EU Member Government states its case to U.S. prosecutors but does not push it vigorously.

This may change as the Wassenaar Arrangement papers over major disagreements on how to control exports to old Cold War targets, such as the People's Republic of China, for which the U.S. imposes strict controls but the EU does not. There has yet to be a major reexport enforcement case involving an export by a European company to China of an item that violated U.S. but not EU law. **Also, the United States has increasingly asserted in-country transfer**

---

[1] In addition, several other U.S. laws also may apply extraterritorially to activities of U.S.-owned or controlled subsidiaries and branches organized under foreign laws. These laws include the antiboycott rules and regulations administered by the Internal Revenue Service and by the Commerce Department, the Foreign Corrupt Practices Act, and various sanctions and embargoes currently administered by the Treasury Department with respect to Cuba, Iran, Sudan, and others. Each of these laws applies somewhat differently. Some (such as the Sudan sanctions) apply to foreign branches and U.S. citizens but not to foreign subsidiaries. Others (like the Iran and Cuba sanctions, and the antiboycott rules) apply to both types of entities. Also, some of the end-user and end-use controls of Part 744 of the EAR apply to activities of "U.S. persons" outside of the United States regardless of whether there is an export or reexport of any U.S. content.

 bflowe@bcr-dc.com

restrictions, the future impact of which may result in new trade disputes.

When major international disagreements arise, they can result in some tempering of U.S. extraterritoriality. For example, a raging international legal debate resulted when the United States prosecuted several European countries for violating the U.S. unilateral controls on participation in the Siberian Pipeline in the early 1980s. Those cases ultimately were settled before international courts could resolve them. Many European and other businesses began openly "designing out" U.S. products to avoid U.S. reexport controls. U.S. industry persuaded the U.S. Government to establish new *de minimis* rules and other exceptions to the extraterritorial application of U.S. law described in this paper. Similar European efforts to design out U.S. satellite components have led to some revisions in the Internaltional Traffic in Arms Regulations ("ITAR") controls to which U.S. satellites were subjected again (although there is a proposed rule to move satellites back to control under the EAR, as discussed in Section 13 below). The overwhelming number and types of U.S. unilateral sanctions, such as the controversial Helms-Burton Act, the Iran-Libya Sanctions Act, and the Comprehensive Iranian Sanctions, Accountability, and Divestment Act of 2010, contributed to the development of a sanctions reform movement in the U.S. business community and in Congress with the objectives of rationalizing the sanctions imposition process and limiting sanctions to instances in which they have a chance to succeed. The Clinton, Bush, and Obama Administrations and a majority of the U.S. Congress have not yet supported meaningful reforms, except with respect to limited agricultural and medical exports and recent liberalization of Cuba travel and remittances restrictions. Significant reform will take time, and reasoned arguments are much more difficult than emotional reactions to terrorists and rogue nations that result in these laws. Also, while non-U.S. exports are subject to some exceptions under U.S. law, for good reasons, one should recognize that these exceptions can also raise U.S. political concerns when politicians perceive that they provide non-U.S. companies with a competitive advantage over U.S. companies.

The American Bar Association Committee on Export Controls and Sanctions, of which I was Chair, authored a resolution against extraterritorial application of export control laws for foreign policy purposes. The arguments in that resolution are useful to cite and hopefully will have some influence if promoted in various fora. *See* http://www.abanet.org/intlaw/regulation/export_rec.html.

The "bottom line": Defending a charge that U.S. extraterritorial laws are illegal under international law would make a great case for us lawyers, but it is generally far more cost effective for businesses to comply with U.S. laws regardless of how distasteful that may be. As the U.K. Government once warned in an official export control publication, "although we view the U.S. claim to jurisdiction as illegal under U.K. law, the U.S. Government commonly penalizes foreign companies who violate such U.S. laws by denying them access to U.S.-origin products and by penalizing any U.S.-based assets."

3. Basic Guidance for U.S. Reexport Control Compliance.

U.S. laws and courts still consider exporting to be a privilege, not a right. Consequently, all exports technically require some type of a "license" or other form of legal authorization. These authorizations are in two forms: (1) "general licenses", "license exceptions", or "exemptions", and (2) "specific licenses", or just "licenses".

"General Licenses", "License Exceptions", or "Exemptions" authorize by regulation the

 bflowe@bcr-dc.com

export of certain items to certain countries without requiring the exporter to apply for written permission. "Specific Licenses," also referred to simply as "Licenses," require the exporter to apply for and obtain written approval from the appropriate U.S. government agency in advance of the export. Thus, if no license exception, general license, or exemption is available, the exporter must apply for a specific license or a license.

U.S. export controls apply not only to reexports of U.S.-origin products, technology, and software, but also to exports from outside the United States of non-U.S.-made products that incorporate more than a minor amount of U.S.-origin content, and in some cases to exports from outside the United States of non-U.S.-made products that are derived from U.S.-origin technology. These extraterritorial controls apply to the consternation of U.S. allies, and the United States penalizes companies for violating them.

For each export transaction (or applicable reexport transaction), the proper basic determinations to be made are as follows:

a. What set of U.S. (and non-U.S.) export controls apply?

b. Is a License required, or does a General License, or License Exception or Exemption apply? If the latter, certify the applicability of the exemption, comply with any conditions set forth in the regulations, and follow appropriate internal procedures to document the legality of the shipment.

c. If the item is not otherwise exempt or authorized, determine to which agencies to apply for requisite licenses, take appropriate steps to prepare and submit appropriate applications, and make shipments pursuant to appropriate export clearance procedures.

Additionally, exporters should employ certain screening procedures as well as export clearance procedures to ensure the legality of all exports, and accurate records must be maintained. The Steps for using the EAR (Section 732) discussed in Part 4 below augment this basic guidance.

4. <u>Reasons for Export Controls and Applicable Multilateral Regimes</u>.

The reasons and justifications for export controls vary with the nature of the items to be exported and the destinations involved. Controls to protect **National Security** have applied to many exports dating back to the Cold War, and are the basis for both the Wassenaar Arrangement multilateral export controls, as well as its predecessor, the Coordinating Committee for Multilateral Export Controls ("COCOM"). National security controls are the basis for the Wassenaar Arrangement also, the goals for which are much more fuzzy than was the case for pre-90s COCOM. The purpose of COCOM was to prevent or delay certain Warsaw Pact and other communist countries from gaining access to advanced equipment or technology that could jeopardize the national security of the United States and its allies. A similar rationale, though with less clear targets and rules, forms the basis for the today's Wassenaar Arrangement, though the countries and regions of instability that are targeted are less sophisticated than the Warsaw Pact, and there is disagreement on how restrictive the controls should be.

Nonproliferation concerns form the basis for post-Persian Gulf War I restrictions on the export of certain articles related to nuclear, missile technology, and chemical/biological weapon

 bflowe@bcr-dc.com

activities to particular countries and end-users as well as restrictions on related activities of U.S. persons. Other **U.S. foreign policies** often provide a more nebulous rationale for controlling exports to specific countries as a means of expressing U.S. disapproval of a country's practices. For example, Sudan and Syria are subject to foreign policy controls because the United States believes these countries support international terrorism. OFAC and antiboycott controls are also the result of foreign policy export controls, as are most munitions controls. Finally, some exports, such as oil, are controlled due to their **short supply**.

Understanding the reason and rationale for particular controls can help exporters determine whether a license is likely to be granted, and to make stronger arguments for approval, such as including appropriate limitations that might allow the export to occur and demonstrating how the purposes of particularly sensitive controls will still be satisfied. For reexports in particular, the applicable rationale can support arguments for approval. For example, one might argue that the United States should not assert tighter controls over a reexport under multilateral export controls than another government does. On the other hand, one can also assert that the United States should not apply purely symbolic foreign policy controls on an extraterritorial basis at all. Remember, though, that these may be better arguments for why a license should be approved than for why it is not needed.

4.1. National Security Controls: Wassenaar Arrangement as COCOM Successor.

COCOM was formed as a classified agreement among NATO Member countries, less Iceland, plus Japan, to control exports to Warsaw Pact countries during the Korean War and the Cold War. COCOM operated on a principal of tight export controls on transfers of military critical technologies in an effort to maintain NATO's technological lead time advantage to counterbalance the Warsaw Pact's advantage in military personnel and weapons. At the time of its demise on March 31, 1994, COCOM also included Australia, and many other countries had agreed to adopt COCOM-like controls (Austria, Finland, Hong Kong, Ireland, New Zealand, Switzerland, Sweden, and South Korea). COCOM operated by agreeing on three basic lists of controlled products and technologies: the International Munitions List, the Atomic Energy List, and the International List of Dual-Use Items that could have a military use as well as a predominantly civilian use. The latter was the principal focus of COCOM and debate therein. COCOM member representatives reviewed export license cases submitted to them by the members under a rule of unanimity, which effectively gave every member country veto power over export licenses, which was frequently exercised when advanced technologies were involved.

Technological innovations far out paced the bureaucracies, as did the thawing of the Cold War with German reunification, the breakup of the Soviet Union, and heightened concerns over nonproliferation as a result of the First Persian Gulf War with Iraq. Russia and other former Soviet republics complained that COCOM was a barrier to building new and better post-Cold War relations. COCOM members agreed to include the former Warsaw Pact countries in a vaguely defined COCOM Forum discussion group commencing in June 1991. This Forum encouraged Russia and other newly independent states to develop export control regimes and qualify to become members of a COCOM successor. COCOM members agreed to disband as of the end of March 1994 and to negotiate to develop a successor regime, with Russia to be a founding member.

The focus of the successor regime, named the Wassenaar Arrangement ("WA") for the small town in the Netherlands where it was founded, is to contribute to regional and international

 bflowe@bcr-dc.com

security and stability by promoting transparency and responsibility in transfers of conventional arms and related dual-use items. More specifically, but not stated squarely, it is to deny conventional weapons and related dual-use items to certain rogue countries and to regions of instability. It does not (as yet) incorporate the other nonproliferation regimes discussed below. Although that would seem to be a logical long-term goal, it has not been pursued given the clearer focus of the other regimes. The United States proposed and most nations informally agreed at the creation of the WA on an unofficial target list to address terrorist supporting nations and the four rogue states of Iran, Iraq, Libya, and North Korea, but there were and remain no clear targets. Unlike with COCOM, WA member countries do not have veto rights, only reporting requirements and loose agreements as described below. The focus of the regime is less clear than was the focus of COCOM, but the United States and others are pressing for increased precision as WA operates over time.

At its creation, the WA consisted of 33 member states; since then, the WA has expanded to 41 member states. The two most difficult problems of formation were the inclusion of Russia and other former Warsaw Pact allies and control over conventional weapons, especially to Iran. Russia publicly agreed several times to halt new arms sales to Iran and to wind down current contracts, but implementation has been fraught with disagreements. Allies also have had difficulty with U.S. proposals to control conventional weapons given that the United States is the world's biggest arms exporter and is proposing to cut off markets of other traditional customer countries. Russia and other newly independent states are being aided by former COCOM members in developing indigenous export control regimes and have become members since they are supplier nations of weapons and other items of concern. The People's Republic of China is unlikely to qualify for some time, if ever, unless it begins to engage in developing effective export controls of its own. China has recently enacted regulations to control chemical, biological, and missile technology, in accordance with its participation in the Nonproliferation regimes discussed below, but its controls for Wassenaar items and the effectiveness of the implementation of these other controls are still of primary concern to U.S. policymakers.

The members agreed on a Basic List of items to be controlled at the national level by, and at the discretion of, individual member states. A subset of that list is a Sensitive List of items subject to tighter controls and greater review and scrutiny, and a smaller subset of the latter is a Very Sensitive List. Consensus of the members is required to change the list. The WA Basic List is described in the EAR by the part of the Commerce Control List subject to National Security ("NS") controls. The Sensitive List (Annex 1 to the WA Agreement) is a subset of the Basic List, and affects reporting requirements under Part 743 of the EAR. EAR Part 743 lists items on the Sensitive List. The Very Sensitive List (Annex 2 to the WA Agreement) is a further subset of Sensitive List. The United States has removed License Exception availability for items on the Very Sensitive List. Accordingly, the United States needs to obtain changes in the WA to authorize License Exception exports of such items. See provisions for License Exception GOV (EAR 740.11) for the ECCNs that are covered in part by the Very Sensitive List. WA Member Countries are committed to exercise "extreme vigilance" in licensing Very Sensitive List items.

All WA Member Countries must report to the WA: (a) the aggregate total of Basic List Denials; (b) the aggregate total of Sensitive List Approvals; and (c) Individual Sensitive List Denials. Reporting does not share information on the exporter's name and address or the dollar value of the applicable items. A confidentiality agreement protects information sharing under WA reporting. WA Members must review others' Sensitive List denials. If a member agrees with a WA Member denial, they will deny the same item to the same end-user. This is a much

 bflowe@bcr-dc.com

weaker arrangement than the United States had sought. In order to exercise leadership and demonstrate fidelity to the WA, the United States is more likely to follow denials than are other members. The United States may thus remove License Exception eligibility by *Federal Register* notice regarding certain items for certain end-users.

On January 15, 1998 and after other member WA nations, the United States implemented the WA changes to the Commerce Control List, and moved old controls to the unilateral controls on embargoed and terrorist supporting countries. However, most target countries in the EAR remain the same as during the COCOM days, and include many WA members (such as Russia) as well as China. It remains to be seen what real effect, if any, the WA regime will have on U.S. exports in the long run. Given the lack of consistency in application of the controls to countries such as China, the list review perhaps has had the most significant effect on U.S. exporters. Once control lists are established, they become vested with an aura of importance and are often used to control items in ways that were not originally intended.

At this time, the EAR (though not the WA) still largely reflects the old COCOM targets. For example, Country Group A:1 to EAR Part 740 still simply lists the old COCOM and COCOM Cooperating Countries, and Group D:1 lists the old COCOM targets. Issues for future consideration include: (a) changes to EAR § 742.4 (National Security controls) to reflect WA instead of COCOM focus; (b) changes to EAR § 742.6 (Regional Stability controls); and (c) adjustments to Country Groups and, perhaps, License Exceptions to reflect current policy. For example, BIS has moved some former Warsaw Pact countries that are members of the EU and/or NATO from Country Group D:1 to B in recent years.

4.2. Nuclear Controls: Nuclear Suppliers Group.

U.S. nuclear export controls are partly derived from and supplement international nuclear export controls that have been perhaps some of the most effective export controls. These export controls supplement more critical nuclear policies of the vast majority of countries that do not have nuclear weapons and the few that do, the Nuclear Non-Proliferation Treaty and regional treaties, and safeguards of the International Atomic Energy Agency ("IAEA") in preventing the spread of nuclear weapons. Many believe that export controls are the least useful of these elements, given the spread of technology and the relative ease of building a weapon now.

In 1975, the United States organized a group of nuclear supplier countries, now formally known as the Nuclear Suppliers Group ("NSG"). This group in 1976 drew up guidelines aimed at supplementing the Nuclear Nonproliferation Treaty and the International Atomic Energy Safeguards. An earlier regime was criticized because it had allowed some nations (India) to circumvent IAEA safeguards and essentially construct nuclear facilities indigenously by copying or modifying technology acquired legally under IAEA safeguards. As a result, the NSG control list broadened the definition of "proliferation" to include the spread of the ability to make nuclear weapons, thus focusing more on technology.

After the first Persian Gulf War with Iraq warned the world of the danger of unstable regimes obtaining nuclear power, NSG nations were reenergized. The NSG Dual-Use Regime was formally adopted by 29 member countries on March 31, 1992. The NSG agreed on a more stringent common policy of restraint in transfers and retransfers from nuclear states to any non-nuclear weapon state of dual-use commercial items that also have uses with nuclear material, equipment, and technology The NSG export control policies are based on two documents, the

NSG Guidelines and the NSG Annex.

The NSG Guidelines set out the purpose of the regime and its basic principle, that NSG members "should not authorize transfers of equipment, material or related technology identified in the Annex for use in a non-Nuclear-Weapon State in a nuclear explosive activity, or an unsafeguarded nuclear fuel-cycle activity, or in general, when there is an unacceptable risk of diversion to such activity, or when the transfers are contrary to the objective of averting the proliferation of nuclear weapons."

The Guidelines require NSG members to establish export licensing procedures for Annex items. While NSG member countries did not agree to formal license review as COCOM had done, the NSG does include information sharing procedures and an important "No Undercut Rule", an agreement among members that if one country denies a particular export license in accordance with the Guidelines, the other members will not take advantage of the sales opportunity to approve similar sales to the same destination. So far, nuclear controls have had strong multilateral discipline for the most part.

Significantly, the United States was unable to persuade NSG members to adopt controls on exports of computers used for nuclear nonproliferation purposes. Other countries believed that general purpose computers have at best an indirect connection with nuclear weapons activities. Accordingly, the United States imposed these controls unilaterally when it published the harmonized Nuclear Referral List in 1994. (Several commentators have argued that the U.S. Nuclear Referral List includes other unilateral controls and is otherwise not fully "harmonized" with the NSG Annex).

NSG Member countries are those included in Country Group A:4 in Supplement 1 to EAR Part 740. In contrast, the countries listed in Group D:2 are of greatest nuclear concern. These are countries that have not signed one of the two international Nuclear Nonproliferation Treaties, and they include some countries that also happen to be close U.S. trading partners, such as Israel, India, and Pakistan. This list is revised from time to time as countries such as Argentina, Brazil, and South Africa have signed the Nuclear Nonproliferation Treaty or the Treaty of Tlatelolco and agreed to adhere to IAEA safeguards for their nuclear power programs.

4.3. Missile Technology: Missile Technology Control Regime.

On April 26, 1987, the United States and six other countries (Canada, France, Germany, Italy, Japan, and the United Kingdom) created the Missile Technology Control Regime ("MTCR") to limit proliferation of missiles that were "capable of delivering nuclear weapons". In January 1993, the MTCR significantly expanded its scope to include more prevalent smaller missile systems capable of delivering chemical and biological weapons. Since 1987, the MTCR has expanded to 34 member countries which have a plenary meeting annually. The MTCR agreement is based on two classified documents, the MTCR Guidelines and the MTCR Annex. The Guidelines set out basic licensing policy, procedures, and review factors, and require standard form government assurances to prevent proliferation and transfers to destinations of concern.

The Annex contains twenty missile-related goods and technologies, which are included as part of numerous entries on the EAR Commerce Control List. The International Traffic in Arms Regulations ("ITAR") also cover Annex items. The Annex consists of two categories of missile-

 bflowe@bcr-dc.com

related goods and technologies, and certain legislative sanctions are based on those categories:

- Category I covers missile systems capable of delivering at least a 500 kilogram payload to at least a 300 kilometer range (*i.e.*, the nuclear payload capable missiles) and the major subsystems and production equipment for such missiles; and

- Category II covers materials, components, production, and test equipment, as well as missile systems with a 300 kilometer range regardless of payload, and major subsystems thereof.

Current MTCR Member countries are set forth in Country Group A:2 in Supplement 1 to EAR Part 740. Countries of concern are set forth in Group D:4.

MTCR List Items, or "MT" controlled items, require a license for export from the United States to all destinations except for Canada. In 2005, BIS proposed eliminating License Exceptions for MT controlled items to Canada, but that proposal was never finalized.

Also, as a result of MTCR changes, BIS broadened the catch-all rule in late 2004 to make it worldwide and applicable to Category II as well as Category I missile activities, and in May 2007, modified ECCNs 1A102, 1C101, 1C107, 6A108, 6B108, 7A102, 7A103, 9A111, and 9B105, all of which used the term "missile", which is defined to include rocket systems and unmanned air vehicles ("UAVs") capable of delivering at least 500 kilograms payload to a range of at least 300 kilometers. These ECCNs were modified to include rocket systems and UAVs capable of a range of at least 300 kilometers, regardless of the payload capacity.

4.4. Chemical and Biological Weapons: Australia Group and Chemical Weapons Convention.

After a finding by the U.N. Secretary General that Iraq had used chemical weapons against Iran in violation of the Geneva Protocol, and that Iraq had obtained the materials for its chemical weapons program from open sources in the international chemical industry, the United States and a number of other governments imposed controls on the export of chemicals used in the manufacture of chemical weapons. In 1985, Australia proposed that these countries meet to harmonize those controls and enhance cooperation among themselves on the issue. The Australia Group thus formed as an informal forum of countries that cooperate to curb the proliferation of chemical and biological weapons and related items by agreeing to harmonize export controls, exchange information, and through other means. The Australia Group meets biannually.

Membership consists of countries identified in Country Group A:3 in Supplement 1 to EAR Part 740. Countries of concern are set forth in Group D:3.

Australia Group members have agreed to impose multilateral export controls on a list of precursor and intermediate chemicals used in the production of chemical weapons, certain microorganisms and toxins, certain dual-use equipment that can be used in the production of such items, and related technology. The Australia Group also serves as a forum for member countries to work together to harmonize licensing and export control procedures to facilitate legitimate chemicals trade without increasing the risk of potential weapons production.

 bflowe@bcr-dc.com

U.S. companies seeking to export listed chemicals and equipment usually do not need a license for export to Australia Group countries or to NATO members but will need a BIS license to export elsewhere. Like the NSG, the Australia Group members do not review license applications, but do share information and have a similar "No Undercut Rule". The U.S. controls are spelled out in EAR §§ 742.2 and 744.4. The United States also imposes controls on activities of U.S. persons and exports of items and technology not on the Australia Group list if they are likely to be used directly in chemical or biological weapons activities. This "catch-all" rule was broadened in March and April 2005 to apply worldwide.

The **Chemical Weapons Convention ("CWC")** entered into force on April 29, 1997 and was implemented in the United States in 1998. This gave the government the authority to enforce the CWC's provisions with respect to private facilities in this country. As of 2012, 189 countries have ratified or acceded to the obligations of the CWC.

The CWC bans the development, production, possession, transfer, and use of chemical weapons. It is enforced through a system of required industry declarations and government on-site inspections. Many chemicals used to make weapons have legitimate commercial applications as well. Therefore, the CWC, for regulatory purposes, categorizes controlled chemicals into three schedules based on the extent to which they have been stockpiled as warfare agents, how easily they could be converted to warfare agents, and the extent to which they are used by industry for legitimate purposes.

- Schedule 1 includes known chemical warfare agents and their precursors, for which there are few uses other than as warfare agents.
- Schedule 2 includes substances used in small quantities by industry.
- Schedule 3 chemicals are those widely used by industry.

Finally, the CWC also has a basket category of unscheduled discrete organic chemicals, which are also widely used by industry.

The CWC restricts exports of Schedule 1 and 2 substances to CWC signatory countries. Export of Schedule 3 chemicals to non-CWC countries is permitted but requires end-use certificates.

The CWC treaty applies only to chemicals and not equipment or technologies. Therefore, Australia Group controls continue to play a critical role in limited the proliferation of chemical and biological weapons.

The CWC Regulations ("CWCR"), implemented in 1999, set forth the obligations of U.S. industry to report to the U.S. Government information on production, consumption, processing, importing, and exporting of toxic chemicals and chemical weapon precursors. Other reporting deadlines are set forth in the CWCR and on BIS's CWC Home Page which can be accessed through the agency's web site (www.bis.doc.gov).

The CWCR also include provisions to allow on-site inspections of private industry facilities by the Organization for the Prohibition of Chemical Weapons ("OPCW"), to verify compliance. The OPCW is the international regime charged with implementing the CWC. The

 bflowe@bcr-dc.com

OPCW chooses Schedule 1 and 2 facilities for inspection based on the level of risk they pose to the objectives of the CWC. Schedule 3 and Unscheduled Discrete Organic Chemical ("UDOC") facilities are apparently chosen by lottery. Since the CWC entered into force in1997, the OPCW has carried out hundreds of inspections in all countries, some of which involved facilities of foreign subsidiaries of U.S. companies. Inspections by OPCW of private facilities in the United States began in 2000.

4.5. The Tension Between Export Controls, Export Promotion, Balance of Trade, and Free Speech.

U.S. export control laws are constantly in flux because of the inherent tension between (A) fundamental reasons for controlling exports, such as national security, nonproliferation of weapons of mass destruction, and foreign policies, on the one hand; and (B) similarly fundamental reasons for making exports, such as the balance of trade, jobs, preservation of industry, free trade, follow on servicing and other business, preserving U.S. businesses' image as a reliable supplier, and at times, freedom of speech. The shifting composition of various export controls is determined by competing ideas and policies, balancing on the fine specifications of a microchip.

The balance between these competing policies shifts from time to time. For example, in the 1980s President Reagan tightened controls because of a perception that high technology was flowing to Warsaw Pact countries at a dangerous rate. Later, as the Cold War was ending, the Trade Promotion Coordinating Committee, chaired by the Commerce Department, acknowledged that the importance of export promotion to the nation's economy was as vital an interest as national security, and asserted a greater policy role for economic considerations. This inherent tension is often evident in disputes regarding license applications and decontrol between the different government agencies that review such matters. The pendulum seems to be now shifting towards relaxing controls, as exemplified by the Obama Administration's Export Reform Initiative. These efforts are driven in part by concerns that the byzantine U.S. system of export controls is broken and that excessive controls over lower-level technologies that are available outside the United States diminishes the ability to adequately protect items that are truly vital to U.S. national security and capable of being controlled. The efforts are also fueled by practical considerations, such as harsh economic realities after the 2008 recession and a desire to promote U.S. exports. The reform efforts are discussed in more detail in 13.1 below. The fundamental competing policies at stake will continue to make export controls dynamic and interesting but difficult to predict.

5. Which Laws and Agencies Govern.

The particular U.S. agency that governs an export will depend on the article to be exported and on the destination. The three agencies that affect most companies are:

- the Bureau of Industry and Security ("BIS") within the Commerce Department, which administers the Export Administration Regulations ("EAR", 15 C.F.R. 730 et seq.) under the Export Administration Act (See website at http://www.bis.doc.-gov/);

- the Directorate of Defense Trade Controls ("DDTC") within the State

 bflowe@bcr-dc.com

Department, which administers the International Traffic in Arms Regulations ("ITAR", 22 C.F.R. 120 et seq.) under the Arms Export Control Act (See website at http://www.pmddtc.state.gov); and

- the Office of Foreign Assets Controls ("OFAC") within the Treasury Department, which administers various embargo and sanctions regulations (31 C.F.R. Part 500 et seq.) under the International Emergency Economic Powers Act, the Trading with the Enemy Act and a number of laws targeting specific countries (see website at http://www.treas.gov/ofac).

Every exporter of U.S. related products will have to address at least one of these sets of export controls, if not all three. Civilian, "dual-use" items generally fall under the export control jurisdiction of the Commerce Department, while military items generally fall under the export control jurisdiction of the State Department. The distinction between civilian and military articles is often unclear, and many items that appear to be civilian in nature are in fact controlled by the State Department. Conversely, as a result of export control reforms, more and more military items are transitioning to control under the Commerce Department's EAR. Consequently, exporters must first examine the control lists of both sets of regulations to determine which agency has jurisdiction. In certain instances, OFAC will have jurisdiction because the destination is embargoed. OFAC shares export control jurisdiction with BIS (and to a lesser extent with DDTC) to varying degrees, depending on the sanctions program, at time asserting priority and at other times deferring to BIS.

5.1. Commerce Department Export Administration Act for Dual-Use Items.

By far, BIS administers the most wide reaching and generally applicable export control regulations (albeit with the advice and consent of the Departments of Defense, State, Treasury, Energy and other agencies, as necessary). The other licensing agencies described below implement more specialized controls. The EAR covers everything that is not under the exclusive export control jurisdiction of one of the other agencies, and covers some that other agencies control as well. Because the other sets of controls are more specialized they are not always mutually exclusive, and there is a great deal of overlap and opportunity for confusion.

The Export Administration Act of 1979, as amended (the "EAA"), authorizes the President to control exports of dual-use goods and technology. Controls are implemented for a variety of policy rationales, such as national security, foreign policy (including preventing proliferation of nuclear, chemical, and biological weapons and missiles to deliver them), antiterrorism, regional stability, and short supply where necessary to protect the domestic economy from the excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand (mostly applicable to oil).

The EAA also controls reexports from other countries of U.S.-origin controlled items as well as exports from abroad of controlled non-U.S.-made items containing at least 10-25% (depending on the destination) U.S. parts and components, and to some destinations the non-U.S.-made direct-products of U.S. technology. U.S. reexport controls have been very controversial, and U.S. allies such as Britain, France, Canada, and Mexico have at times imposed "blocking orders" forbidding their nationals (including subsidiaries of U.S. companies) from complying with U.S. foreign policy reexport controls that are at odds with their own country policies.

 bflowe@bcr-dc.com

Congress and the Administration have been trying for years to revise the Cold War era EAA to replace its artificial foreign policy versus national security distinctions and modernize it to reflect current geopolitical concerns over proliferation of weapons of mass destruction and regional stability. These efforts have been mired in controversy over issues of export control administration (whether Commerce or Defense, State, or other agencies should have the lead role and to what extent) and the degree to which controls should be liberalized or strengthened. There have been several attempts to reform the EAA over the years, but none so far have achieved the necessary consensus of both houses of Congress and the president. It remains to be seen whether new export control legislation will emerge during a second Obama Administration.

Since the EAR has technically expired, President Obama's Administration (like that of Bush and Clinton before it) continues to administer the export control laws under Executive Orders issued pursuant to the broad authority of the International Emergency Economic Powers Act ("IEEPA"), in effect pretending the EAA is still in force. This has created some legal difficulties, but has had little practical effect on most exporters.

While revision and reauthorization of the EAA has proven difficult, drastic increases in penalties for export control violations have been ushered in with relative ease in recent years. Since 2006, civil penalties for violations of the IEEPA have increased from $11,000 up to the greater of $250,000 or twice the amount of the transaction value. The maximum criminal monetary penalty per IEEPA violation is $1,000,000.

5.2. State Department Arms Export Control Act for Munitions.

The Arms Export Control Act of 1976 ("AECA"), as amended, authorizes the President to control exports and imports of defense articles and services. Its purpose is to promote world peace, national security, and U.S. foreign policy by restricting the worldwide availability of certain articles and technology. The International Traffic in Arms Regulations ("ITAR") (22 C.F.R. § 120 et seq.) implement the AECA. The Directorate of Defense Trade Controls ("DDTC") within the State Department administers the ITAR.

The ITAR in fact have governed exports of much more than items traditionally thought of as "arms", such as certain electronics and electronics systems. For example, until 1996, the ITAR governed exports of most commercial encryption software, and the ITAR still governs exports of commercial satellites, though there is movement afoot to change this. Like the EAR, the ITAR cover technical data and software as well as commodities. However, there are important differences between EAR and ITAR controls and licensing procedures. For example, a company planning to provide "defense services" to a foreign entity must first submit a proposed agreement to DDTC for approval even if it is not exporting technology or commodities. Also, virtually everything on the ITAR requires a license for export to most countries, although DDTC has published a growing number of exceptions and authorized broader latitude under certain approved types of transactions in recent years, to help U.S. defense companies remain competitive internationally.

Defense articles and services are those items identified on the U.S. Munitions List ("Munitions List"). DDTC generally designates items for inclusion in the Munitions List when the article, service, or technical data:

- is specifically designed, developed, configured, adapted, or modified for military

 bflowe@bcr-dc.com

application; and

- has significant military or intelligence applicability; and
- does not have predominantly civil applications; and
- does not have performance equivalent (defined by form, fit and function) to those of an article or service used for civil applications; or
- is specially designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability warranting its control.

Exporters should consult the Munitions List for exports of any commodities that could fall within the Munitions List Categories. If an article is described on the Munitions List, its intended end-use, whether civil or military, is irrelevant.

The issue of commodity jurisdiction has been the subject of much debate. The debate has been hampered by State and Defense Department officials' mistrust of the Commerce Department's ability to control exports. Between 1991 and 1996, the two agencies transferred several whole categories of items from State/ITAR to Commerce/EAR export control jurisdiction (including most encryption software and hardware, some civil satellites, and a commercial encryption software). The debate on commodity jurisdiction procedures was a key stumbling block to the attempted passage of Export Administration Act renewal legislation in the fall of 1994. As a result, the Clinton Administration established new procedures in 1996 to address commodity jurisdiction issues, giving agencies the right to escalate controversial cases for decision at the White House level (i.e., to the National Security Council). These procedures did not work very efficiently and have since been further revised. In the late 1990s, after concerns over certain transfers of technology to assist Chinese space launches, Congress transferred export control jurisdiction over commercial satellite equipment from the EAR back to the ITAR, resulting in increased licensing requirements and delays. In the last few years, U.S. export control agencies have had particularly contentious disputes concerning jurisdiction over "space qualified" parts and night vision equipment. The National Security Council has brokered resolution of these disputes.

Normally, DDTC and Commerce's Bureau of Industry and Security ("BIS") representatives will work with company officials to determine which set of regulations govern a particular technology. If there is any question as to whether the product is controlled by the Munitions List or the EAR's Commerce Control List, the exporter should consider filing a "Commodity Jurisdiction Request" with DDTC, with a copy to BIS, to obtain a formal determination (see ITAR § 120.5). The exporter should explain the matter in detail, including a history of the product's design, and should make a case to DDTC as to which set of regulations should apply. Generally, exporters prefer their products to be within the jurisdiction of the EAR because its controls typically are less stringent than those of the ITAR.

Likewise, the ITAR appears to overlap with export controls administered by both the Nuclear Regulatory Commission ("NRC") and Department of Energy concerning certain nuclear materials and assistance, particularly in areas involving nuclear weapons and naval nuclear propulsion. The NRC and Energy Department regulations are found at 10 C.F.R. Parts 110 and

810. In practice, DDTC generally has deferred to both the NRC and Energy if those agencies' licenses would completely cover the same activities for which an ITAR license otherwise would be required. Nevertheless, exporters are advised to consult with these agencies when such overlap is apparent.

5.3. Treasury Department's Embargo and Sanctions Programs.

The Treasury Department through its Office of Foreign Assets Control ("OFAC") administers a variety of trade embargoes and asset freezes against designated "hostile" countries, organizations, and individuals. On occasion, OFAC will also freeze assets of a country to protect them from insurrections or raiding parties, as occurred with the now defunct Kuwaiti Assets Controls. While OFAC restrictions are typically very comprehensive and subject to only the narrowest of exceptions, OFAC will issue general and specific licenses for certain transactions with the embargoed countries if the circumstances permit. However, OFAC representatives have always made clear that licensing certain activities is at best secondary to the agency's primary mission of prohibiting business with the target countries and their nationals. Set forth below in Part 9 is a summary of OFAC controls.

Because they are so comprehensive as to the countries they cover, OFAC controls overlap significantly with controls administered by other agencies. Generally, OFAC asserts primary jurisdiction vis-a-vis the export controls administered by other agencies, but that is not always the case. With the increasing number of embargoes in recent years, the seemingly *ad hoc* scheme of overlap between OFAC embargo controls and the BIS administered EAR and other export control regulations has been quite problematic for exporters. In some cases, an export or reexport license issued by BIS is alone sufficient. In others, only an OFAC license is required. In still others, one must obtain licenses from both agencies for the same or similar transitions. Thankfully, BIS has spelled out this overlap much more clearly in EAR Part 746, though turf battles have inhibited efforts to rationalize their overlapping jurisdictions on a consistent basis. There has been little consistency over the years, and determinations as to which agency has primary authority has been the function of who is in charge of the agencies at a given time as much as any other rationale.

The following chart generally describes which agency has primary export control jurisdiction between BIS and OFAC:

Country	BIS or OFAC Primary
Cuba	BIS for exports and reexports; OFAC for transactions and foreign subsidiaries of U.S. companies.
Iran	OFAC for imports, exports, and reexports; BIS for exports and reexports not prohibited and not licensed by OFAC.
North Korea	BIS for exports and reexports; OFAC for Specially Designated Nationals ("SDNs").
Sudan	Exports and reexports: BIS for CCL items; OFAC for EAR99 and CCL items (i.e., 2 licenses for CCL items).
Syria	BIS for exports and reexports; OFAC for blocked assets.

 bflowe@bcr-dc.com

One should consult with OFAC, BIS, and other relevant agency officials, the regulations, and practitioners for precise details. While it has been rare for one agency to enforce the law against a company that only obtained a license from the other agency, one should not be lulled into complacency. Such enforcement is likely if one willfully fails to obtain all applicable licenses as opposed to failing to obtain one due to confusion.

Overlap of OFAC regulations with those of other agencies has rarely been a problem due to the fact that companies rarely bother to apply for licenses to export to embargoed countries munitions, nuclear energy, or other more specialty regulated items.

See further discussions below on recent changes to the Iranian and other sanctions.

5.4. Other Specialty Export Control Agencies and Laws.

In addition to BIS, DDTC, and OFAC, at least ten other federal agencies control exports in some way, and a number of other regulations have related effects on exporters. These include export control regulations administered by the Nuclear Regulatory Commission (nuclear items) and Department of Energy (nuclear technical assistance), Maritime Administration, Environmental Protection Agency, Drug Enforcement Agency, Agriculture Department, Fish and Wildlife Service, Patent and Trademark Office, Food and Drug Administration, and Consumer Product Safety Commission. In addition, the U.S. antiboycott regulations, Foreign Corrupt Practices Act, Defense Department Industrial Security Regulations, and the Bureau of Alcohol, Tobacco and Firearms and Explosives import and manufacturing regulations can affect exporters. These specialty agencies are beyond the scope of this seminar, but deserve mention.

5.5. Need to Address Agencies Other Than Commerce.

Most compliance programs omit any reference to agencies and regulations other than BIS and the EAR. Given the potential of coverage by other controls, compliance programs should at least refer to the OFAC and ITAR controls, and export administrators should have access to them (or to specialists who can advise whether they apply). If a problem occurs with regard to other regulations, the agency will look with disfavor if it has been ignored in export compliance procedures.

6. Export Administration Regulations.

The EAR were revised in 1996 to make them clearer and more straightforward. Nevertheless, it is impossible to summarize clearly what remains a six-inch thick binder of detailed rules and regulations. Described below are the 10 basic prohibitions, basics of license exceptions, how export compliance administrators should develop a product country matrix to determine when licenses are needed due to product technical specifications, and basic screening procedures to ensure that licenses are not required due to the end-use or end-user for particular exports.

6.1. Export Control Factors of Concern.

In order to determine whether a license is required for a given export, one must determine the following:

 bflowe@bcr-dc.com

- the Export Control Classification Number of the product according to the Commerce Control List, a complete and detailed listing of control parameters by which one determines when a license is required to export products with particular specifications to which countries;

- the Country of Destination;

- the End-User for the product, as well as any intermediaries who will control the product before it reaches the end-user; and

- the End-Use intended for the product.

In addition, the EAR prohibits certain conduct by "U.S. persons" regardless of whether there is an export if such activities would contribute to the proliferation of nuclear, chemical, or biological weapons, or missiles capable of delivering such weapons, or would further boycotts of countries that the United States does not boycott (mainly Israel).

Many of the prohibitions of the EAR described below will only apply if one has knowledge of the end-user and end-use. Determining whether a corporation has "knowledge" can be difficult. Accordingly, attached hereto is a copy of BIS's "Know Your Customer Guidance and Red Flags," which present the clearest summary of the standard of care to which BIS will hold exporters in determining whether one "knows" what its customers intend to do with products.

6.2. Scope of the EAR.

The EAR covers all items exported from the United States, except certain ones specifically excluded in the EAR. Exclusions from the scope of the EAR mainly involve items that are subject to the exclusive export control jurisdiction of another federal agency, or publicly available technology and software. Publicly available technology and software includes that which is protected by patents, to the extent such technology or software is fully disclosed in patents available in any public patent office, as well as any other technology that is readily distributed at no more cost than the cost of copying. Proprietary data, trade secrets, or any information that a company protects from public disclosure is not exempt from the EAR. Encryption source code (other than in printed form) is specifically not covered by the publicly available exclusion from the EAR, although current encryption controls now provide nearly equivalent authority for export, except to the Country Group E destinations.

The United States also asserts jurisdiction over "reexports" beyond U.S. borders, to the consternation of most U.S. allies who believe international law prohibits such extraterritorial controls. These reexport controls apply to:

- "U.S.-origin" items wherever located

- Foreign made items containing more than a *de minimis* amount of U.S. components (10% for embargoed countries; 25% for others)

- Foreign made items that are the "direct products" of certain U.S.-origin technical data or software, depending on the country to which such foreign made products are shipped.

 bflowe@bcr-dc.com

Note that foreign made technology that is commingled with any U.S. technology is subject to the EAR regardless of the percentage of U.S. technology, unless the non-U.S. reexporter submits to BIS a One Time Report demonstrating why the applicable product contains less than the *de minimis* level of U.S. content. As of October 3, 2008, the One Time Report requirement for software was eliminated. These exemptions are discussed further in Section 8 below.

The EAR increasingly covers in-country transfers of items subject to the EAR as well, despite objections by exporters.

Again, the EAR also covers certain activities of U.S. persons related to proliferation of nuclear, chemical or biological weapons or missile technology, assisting in the development abroad of encryption software, or other activities prohibited by a denial order.

6.3. General Prohibitions.

The EAR contains ten basic prohibitions. The first three are based on the Export Control Classification Number ("ECCN") set out in the Commerce Control List at the end of the EAR. Company export compliance administrators should carefully classify each product and maintain a "Product Matrix" showing the ECCNs of each product. If properly maintained, a Product Matrix should allow personnel easily to determine whether an export license is required or whether a License Exception applies and under what conditions. The last seven prohibitions are based on transaction factors other than the ECCN of the products. The prohibitions are as follows:

Prohibition 1:	**Exporting and Reexporting Controlled Items Having ECCNs Requiring Licenses to Listed Countries without Obtaining Applicable Export Licenses**
Prohibition 2:	**Reexporting Foreign-Made Items Incorporating More than a *De Minimis* Amount of Controlled U.S. Content without Obtaining Appropriate Licenses and without an Applicable License Exception**
Prohibition 3:	**Reexporting to Certain Countries Foreign-Produced-Direct-Products of U.S. Origin Technical Data or Software without Obtaining Appropriate Licenses and without an Applicable License Exception**
Prohibition 4:	**Exporting, Reexporting, or Transferring within a foreign Country to Parties on the Denied Persons List (a list of organizations and individuals that have violated the EAR)**
Prohibition 5:	**Exporting or Reexporting to End-Users Known to be Involved with Certain Sensitive Nuclear Weapons or Energy, Chemical or Biological Weapons, or Nuclear End-Use Activities**
Prohibition 6:	**Exporting or Reexporting Virtually Any Product to Embargoed Destinations (Cuba, Iran, North Korea, Sudan, and Syria (Note that all are under tight restrictions))**

Prohibition 7:	**Engaging in Conduct Supportive of Proliferation Activities Described in Item 5, or Supporting Foreign Persons in Development or Use of Non-U.S. Encryption Items that if in the U.S. Would Be Subject to EAR Controls**
Prohibition 8:	**Shipping Certain Items in Transit Through Former Communist Countries If They Will Be Unladen from Vessels or Aircraft while in Country**
Prohibition 9:	**Violating Any Order, Term, or Condition of a License or License Exception Authorization**
Prohibition 10:	**Proceeding with Any Transaction with Knowledge that a Violation of the EAR Has Occurred or Is About to Occur**

6.4. Commerce Control List and Country Chart.

The Commerce Control List ("CCL") is a detailed listing of all types of commercial items according to the parameters that justify controlling their export to certain countries. This is a complete list, in that items not meeting the parameters specified in ECCNs are covered by the so-called "basket category": EAR99. EAR99 items may be exported to all countries except embargoed countries without the need for a license, using the designator "NLR" for "No License Required," provided that Prohibitions 4-10 do not apply.

An ECCN is a five character code, consisting of a number (0-9), followed by a letter (A-E), followed by a number (0-9), followed by a number (0-9), followed by a number (1-9); e.g. 1A001, 5D992.

All listed products will fall under an ECCN in one of the following CCL categories, represented by the first number in the ECCN:

0. Nuclear Materials, Facilities, Equipment, and Miscellaneous
1. Materials
2. Material Processing
3. Electronics
4. Computers
5. Telecommunications (Pt. 1) and Information Security (Pt. 2)
6. Lasers and Sensors
7. Navigation and Avionics
8. Marine
9. Propulsion Systems, Space Vehicles and Related Equipment

Each category is further subdivided by the second letter: "A" is for products and components, "B" is for test equipment, "C" is for materials, "D" is for software, and "E" is for technical data.

For example, most general purpose computer software is classified under ECCNs in Category 4D (or is EAR99 if not covered by a specific ECCN thereunder). Most telecommunications software is classified under ECCNs in Category 5D (Part 1). Software with

information security functions are generally classified under Category 5D (Part 2). However, certain specialty software is covered by other categories. If a product contains functions that are covered by more than one ECCN, the one with the most restrictive controls applies.

Classification is critical. Each ECCN lists various reasons for control at the beginning of the entry. The reasons for control correspond to the columns in a detailed "Country Matrix" set forth in Supplement 1 to EAR Part 738. Thus, knowing the ECCN and reasons for control is the key to determining whether a license is required, by reference to the Country Matrix. Company export compliance administrators should review these categories against the Country Matrix to determine to what countries they may export applicable products with No License Required (using the designator "NLR"). The ECCN also advises which ones may nevertheless be eligible for export under particular License Exceptions, discussed further below.

Classifications may be made by the company, but exports of controlled products without a required license are strict liability offenses if the company's classification is in error. If in doubt as to the proper classification, one may apply to BIS for a formal classification pursuant to the provisions of EAR § 748.3.

Company export compliance administrators should maintain a detailed Product/Country Matrix showing the results of their classification efforts to show clearly when either: (i) products may be exported under NLR or a License Exception, or when (ii) License Applications must be filed with BIS, go through interagency review, and Licenses issued before an export shipment can be made. Company export compliance administrators and engineers should also work with BIS and other U.S. Government officials to help redefine export control technical parameters to keep pace with advances in mainstream technology.

The applicable CCL entry will also determine whether exporters must report to BIS exports under certain License Exceptions, as described in Paragraph 6.5 below. Reporting requirements are important consequences of some classifications.

6.5. License Exceptions.

Even if the applicable ECCN shows that export licenses are required for certain products to certain destinations, there are several License Exceptions set forth in Part 740 of the EAR that may apply. The applicable ECCN lists some of the available License Exceptions that are determined by the parameters of the product. Others may also be available based on the type of export (such as TMP for certain temporary exports or BAG, which is used by most travelers for their baggage). Each License Exception has specific requirements that must be met before it will authorize the export. The License Exceptions include, among others: ENC for certain encryption commodities and software, TMP for certain temporary exports for demonstration, tools of the trade for exhibition, and baggage, RPL for certain replacement parts that do not enhance the technical characteristics of the previously exported product, GBS for items with certain technical characteristics destined for most "Western" countries, and CIV for most items that qualify for GBS but for civil end-users and end-uses in former East Bloc countries.

6.6. End-Use and End-User Controls.

Even if NLR or a particular License Exception would otherwise apply to a given export, reexport, or in some cases in-country transfer, it is illegal to use such authorization in certain

situations. Thus, it is wise to screen to determine if any of the following prohibitions based on the end-use or end-user apply:

a. Parties on Denial Lists. If the customer appears on any of the lists of Denied Parties issued by U.S. government agencies, including the Denied Persons List and Entity List issued by BIS, and the Specially Designated Nationals lists issued by OFAC, the export will almost certainly require a license. If it is on the BIS Unverified List, it might require a license, depending on the circumstances.

b. Sensitive Nuclear End-Users or End-Uses. If the customer is involved in design, development, fabrication, or testing of nuclear weapons or explosive devices; or design, construction, fabrication, or operation of facilities or components of facilities for chemical processing of irradiated special nuclear or source material, heavy water production, separation of isotopes of source and special nuclear material, or fabrication of nuclear reactor fuel containing plutonium, or unsafeguarded nuclear facilities, the export will require a license.

c. Chemical or Biological Weapons End-Users or End-Uses. If the customer is involved in design, development, production, stockpiling or use of chemical or biological weapons, the export, reexport, or in-country transfer will require a license.

d. Missile Technology End-Uses and End-Users. If the customer is involved in, or the export will be used in any way involving direct or indirect assistance in, the design, fabrication, operation, or maintenance of rocket systems (including ballistic missile systems, space launch vehicles, and sounding rockets), or unmanned air vehicle systems (including cruise missile systems, target drones, remotely piloted vehicles, and reconnaissance drones), the export, reexport, or in-country transfer will require a license.

e. Military End-Users or End-Uses. For License Exception CIV, Iraq (other than to Coalition Forces), certain microprocessors to Country Group D:1, and certain ECCNs to China, exports are restricted to civil end-users and for civil end-uses.

These restrictions (other than the Denial Lists) do not apply to exports to all destinations. See EAR Part 744 for details. Attached is a model screening checklist to assist in screening to avoid exports to unlawful end-users or for unlawful end-uses.

6.7. Export Shipping and Recordkeeping.

Unlike for export shipments from the United States, the strict documentation requirements of EAR Part 758 do not apply to reexports of products from outside the United States. However, the recordkeeping requirements of Part 762 must be followed, and shipping and other records must be made available to appropriate U.S. authorities on demand. As a practical matter, U.S. authorities must work through host governments to obtain records on demand from non-U.S. persons, but companies generally cooperate rather than putting authorities to this task. Certain licenses must be supported by end-user statements, and certain License Exceptions such as TSR and CTP require that one either obtain a written assurance or other statement from a customer, or provide a specific destination control statement on shipping documents.

 bflowe@bcr-dc.com

6.8. Reporting Requirements.

The EAR requires semi-annual reports to BIS about exports under License Exceptions LVS, GBS, CIV, CTP, TSR and GOV of items covered by the "Sensitive List" of the Wassenaar Arrangement ("WA"). Forty-five ECCNs are affected. EAR Part 743 contains a list of the applicable ECCNs and reporting requirements. Reports must be mailed or faxed to BIS twice a year: (a) by August 1 for exports shipped January 1 - June 30, and (b) February 1 for exports shipped July 1 - December 31. Reports for items subject to the requirements (other than computers and assemblies under ECCNs 4A003.b & .c, which are discussed below) must include the applicable ECCN with the paragraph reference, the number of units in the shipment, and the country of ultimate destination. Reports should be submitted on the Multipurpose Reporting Form (Form BIS-742R), although use of said form is optional.

Reporting requirements also apply to other types of exports, notably many types of encryption products exported under License Exception ENC, bulk export licensing arrangements, and computer products exported under License Exception CTP. Industry has been urging BIS to abolish all encryption reporting requirements in view of the WA decision to do so and the costs and administrative burden of reporting. Due to recent liberalization of controls on encryption, discussed further below, semi-annual sales reporting of less sensitive encryption items is no longer required, but an annual report of self-classifications must be submitted.

6.9. Exploration of the "Deemed Export" Rule.

The U.S. high-tech industry, faced with an estimated shortfall of over 400,000 qualified U.S. experts, hires thousands of foreign nationals annually, many from China, India, Russia, and other countries which the U.S. government fears support economic and national security espionage. U.S. companies that hire foreign nationals are required to treat certain technical data provided to them as an "export" under the "deemed export" rule, set forth in EAR § 734.2(b)(2) and (5), and thus must in some cases obtain export licenses from BIS to authorize transfers of technology or source code to their foreign national employees. Deemed export violations carry the same penalties as any other violation of export controls.

As a practical matter, the rule has its greatest impact on employees from countries long considered to be national security risks (like China or Country Group E nationals (i.e., Cuba, Iran, North Korea, Sudan and Syria) since little is decontrolled to them), but it applies to all foreign nationals who have access to technology or source code that would require a license to export to their home country. The deemed export rule is highly controversial and not well understood by most companies. The past several years have seen increased enforcement of deemed export violations by BIS, perhaps due to pressure stemming from critical reports of the Commerce Department Inspector General and high-level BIS attention to the issue that followed.

6.9.1. Development of Deemed Export Rule. In 1994, the Commerce Department, prompted by a few companies' requests for clarification, codified what some officials had advised informally was already the law under the EAR. As a result, the so-called "deemed export" rule was created on March 22, 1994 in current EAR §§ 734.2(b)(2) and (9). This rule treats disclosure of technical data in the United States to foreign nationals as an "export." Thus, when U.S. companies provide domestic access to proprietary technology to foreign national employees (typically H-1, H-1B, L, or F-1 visa holders) and to visitors, they

must make the same export licensing determinations as they do for actual transfers of technical data to overseas destinations.

There is no statutory requirement for the deemed export rule and there have been few enforcement cases in comparison to cases involving actual exports of goods or technology. (The majority of enforcement cases involved additional counts to other traditional export/reexport violations.) However, under the EAR, deemed export violations carry the same penalties as any other violation -- currently up to $250,000 for civil offenses and denial of export privileges, and up to $1,000,000 fine and prison time for criminal violations.

The deemed export rule requires companies to determine to what technical data foreign nationals will have access, then to classify that data under the correct ECCN on the CCL. The applicable ECCN will determine whether a license will be required, or whether the access may be provided with No License Required ("NLR") or pursuant to License Exception TSR (with a written assurance first obtained from the foreign national) or License Exception TSU. Again, to facilitate compliance with the deemed export rule, companies should consider developing a technology matrix clearly setting forth licensing requirements applicable to transfers of corporate technical data to foreign nationals.

Whether Licenses are required often depends on a national's country of citizenship and which of the Country Groups in Supplement No. 1 to EAR Part 740 applies. Licenses will always be required for deemed exports of CCL-listed technology for foreign nationals who are citizens of one of the Embargoed Countries. Licenses will also often be required for foreign nationals of one of Country Group D:1 countries which have been identified as a national security risk, including China, Russia, several former Soviet republics, Iraq, Libya, and Vietnam. Controlled technical data transfers to foreign nationals of countries in Country Group B, such as Germany or Japan, are generally permitted, at least under License Exception TSR, provided that the foreign national first signs a special written assurance that they will not reexport the technology or source code they receive to D:1 or E:1 countries. Thus, it is advisable to have all foreign national employees sign a special nondisclosure agreement that incorporates this type of written assurance.

Some highly controlled technology and source code requires a license prior to "export" to any foreign national from any country (except Canada), such as technology for the development or production of certain radiation-hardened integrated circuits, linear accelerators, mass spectrometers, oscilloscopes, some types of computers, and telemetering equipment. Furthermore, the ITAR require licenses for almost all "Munitions List" technology transfers.

With respect to encryption, there is no longer a deemed export rule for transfers of encryption source code in the United States if one is not aware of a plan for an actual export across borders; therefore, these transfers generally are treated as non-exports. EAR § 734.2(b)(9). (Object code software, also known as binaries, is never subject to the deemed export rule.) While there is a deemed export rule for domestic transfers of encryption technology, these controls do not present the special compliance problems they once did. These issues are discussed in Section 3 below.

Prior to 1994, most exporters believed that the release of EAR controlled technical data to foreign nationals would be treated as an "export" only when the person releasing the technology had knowledge that its recipient intended to export it in fact to his or her home country or any

 bflowe@bcr-dc.com

other country. This "knowledge or intent-based" criterion was the basis of old EAR § 779.1 (b)(1)(c), and is a key element of the current EAR's General Prohibition 10 and the "Know Your Customer Guidelines." U.S. industry has strongly urged the Administration to drop the deemed export rule, a solution that would return to the more subjective pre-1994 knowledge or intent-based rule.

Many U.S. companies believe that the deemed export rule impairs the competitiveness of U.S. industry, unfairly discriminates against foreign nationals, and violates the 1st Amendment right to free speech. With regard to the latter belief, the U.S. Justice Department has reportedly expressed its reservations about the constitutionality of the deemed export rule, which -- at least on its face -- suggests an infringement on the right to free speech inside U.S. borders. Moreover, because BIS requires information on the date and place of birth of foreign nationals and certain other sensitive personal data, U.S. companies are put in a difficult position, as many think they may be prohibited from asking for such information under U.S. anti-discrimination laws. (There are national security exceptions to EEOC laws that allow it.)

If efforts to reform the deemed export rule do not succeed, and it is vigorously enforced, a constitutional defense may make progress through litigation. Companies facing prosecution can certainly raise the First Amendment arguments and possibly overturn the rule. For now, the "deemed export" rule is the law of the land, and companies are better off complying as best they can than risking enforcement efforts. Congress and the Office of Inspector General have urged more, not less deemed export enforcement.

6.9.2. Enforcement of the Deemed Export Rule. Enforcement is carried out by BIS Office of Export Enforcement agents who are stationed in field offices across the U.S. and overseas. OEE agents are increasingly visiting U.S. facilities in order to determine whether they employ foreign nationals, and if so, whether the companies have obtained export licenses for those employees. In addition, OEE began a visa review program in 1996, in which they visit companies after the State Department notifies them of certain foreign nationals who are sponsored in high-tech companies for non-immigrant visas (particularly H-1B or L-1 visas). These visits are disconcerting at best for the companies and their employees.

This program was enhanced by the implementation of a new requirement in the visa application process. Effective February 20, 2011, U.S. employers are required to use a new version of immigration form I-129, "Petition for a Non-Immigrant Worker," which contains a certification of compliance with the EAR and ITAR when sponsoring H-1, L-1, and O-1 visas. The form requires the employer to certify either that an export license is not required, or that the employer will obtain one prior to disclosing any export controlled data. If an incorrect certification is made, an employer faces possible civil and criminal penalties for false statements. Further, in submitting the I-129, employers authorize U.S. Citizenship and Immigration Services to conduct on-site audits and compliance reviews. Violations of the deemed export rule can, of course, also lead to penalties under the EAR and ITAR, including fines, denial of export privileges, and debarment, separate and apart from any immigration violations that may occur.

BIS has also reported in its 2009-2011 annual reports that it has made hundreds of outreach visits per year focusing on deemed export compliance, and followed dozens of leads and cases involving alleged deemed export violations.

 bflowe@bcr-dc.com

Because the deemed export rule is not well understood, some U.S. high-tech companies could be in violation of BIS regulations. Export Enforcement officials have stated that the deemed export rule is a BIS enforcement priority. On October 11, 2000, a federal grand jury indicted Suntek Microwave, Inc. ("Suntek") of Newark, California and Charlie Kuan, president of Suntek, for several export control violations, including one count for releasing microwave technology to three nationals of the People's Republic of China without the licenses required by the EAR. This indictment appears to be the first instance in which civil or criminal charges have been brought against any party for violating BIS's deemed export rule. The deemed exports allegedly occurred in connection with eight other counts in the indictment for unauthorized exports of detector log amplifiers and related data to China. The indictment also set forth charges stemming from such exports against Suntek, Mr. Kuan, Silicon Telecom Industries, Inc. ("Silicon") of Santa Clara, California, and Jason Liao, the owner of Silicon. Because the deemed export count was only one of nine other counts of more traditional export control violations, some export lawyers were concerned that the case may make for bad law if, for example, the defendants did not litigate the constitutionality of the deemed export rule the way they would do if that were the only charge. Still, this enforcement case points out one reason the deemed export rule is not needed. It involves a domestic transfer with knowledge that the recipient would make an actual export in violation of the law, which would violate General Prohibition 10 regardless of the nationality of the recipient. Thus, the deemed export rule was not needed for that count in the indictment against Suntek.

The indictment was hailed by the Office of Export Enforcement and the trade press as evidence that enforcement officials were finally starting to enforce the deemed export rule, at least in egregious cases. Suntek received a $339,000 criminal fine and, in the related administrative case, agreed to pay a $275,000 administrative penalty and to a twenty-year denial of export privileges (although Suntek's administrative penalty was waived). Kuan also agreed to pay a $187,000 administrative penalty and to a twenty year denial of export privileges. (There is also a risk of deportation by the U.S. INS for foreign national recipients involved in unauthorized deemed exports.)

The Suntek case was followed by four non-criminal enforcement cases involving Pratt & Whitney, Fujitsu, Lattice Semiconductor, and New Focus, Inc., all of which arose from voluntary self-disclosures. OEE officials have confirmed that a voluntary disclosure generally results in a presumptive reduction of the maximum penalty by 50%. Despite the fact that all four exporters voluntarily disclosed and were credited with having cooperated fully with OEE investigators, the administrative penalties in these deemed export cases still ranged between $125,000 and $560,000 (even under old maximum penalty amounts of $11,000 or $50,000 per violation). Deemed exports to Chinese national employees were involved in three of the four cases; the Pratt & Whitney case also involved deemed exports to nationals of EU countries.

There seemed to be an uptick of deemed export cases in 2008, although most involved more modest penalties (perhaps because the cases had been initiated prior to the 2007 increase to civil penalty amounts). In May 2008, a $31,500 fine was imposed against TFC Manufacturing, Inc. for deemed exports of ECCN 9E991 aircraft-related technology to an Iranian national employee. In August of 2008, Ingersoll Machine Tools, Inc. settled a seven-count deemed export case for $126,000, which involved the alleged release of 1E001 and 2E002 technology to Italian and Indian foreign national employees in the United States. AMD also settled a two-count deemed export case in August 2008 for $11,000, involving release of 3E002 technology to a

 bflowe@bcr-dc.com

Ukrainian foreign national employee in the United States. All three of these cases involved only deemed export violations.

There have been several other cases where deemed export violations were mixed in with hardware and technical data exports. Another August 2008 settlement involving Reson, Inc. had two deemed export charges added on to six other "acting with knowledge" export violations related to reexports by a foreign affiliate. The penalties in that case were just under $10,000 per violation. Another case was settled in October 2008 with Maxim Integrated Products, Inc. involving both unlicensed exports and reexports of hardware, as well as three deemed export charges involving nationals of China and Iran. The allegations involved deemed exports to two employees, but included an extra count for releasing technology to the Chinese national while a deemed export license application was pending. The average penalty amount in that case was approximately $5,600. An administrative case settled with ArvinMeritor, Inc. in March 2011. That case involved one deemed export violation, eleven violations relating to exports of technical data, and two exports of hardware. The deemed export counts did not appear to be directly related to the other export violations, suggesting that they were discovered in the process of doing an internal investigation relating to the hardware shipment. The average penalty in that case was $7,143.

Perhaps the take-home point in these cases is summed up by comments by Julie Salcido, Special Agent in Charge of the OEE Field Office in San Jose, California at a 2006 conference on technology controls. Agent Salcido remarked that her agents are pursuing deemed export cases since they are easy cases to make, because OEE needs only to establish the nationality of a foreign national employee, and that the national had access to controlled technology. Defending such a case can also involve the formidable task of proving that a foreign national has not had access to controlled technology. Deemed export cases can also result in multiple violations, since each release of controlled information to an employee or visitor can constitute a separate count.

It appears that most defense lawyers are not questioning whether the deemed export rule is an unconstitutional prior restraint on speech by U.S. persons to others in the United States. Perhaps universities, which have been under more scrutiny recently for export compliance, will raise such defenses more readily.

Companies in the United States should review non-immigrant foreign nationals to ensure that all disclosures that might be made to them will be covered by the designator NLR ("No License Required") or appropriate License Exceptions, or that Licenses are applied for and obtained. NLR and License Exceptions TSU and TSR cover the vast majority of deemed exports, but export compliance personnel should ensure that foreign nationals sign Nondisclosure Agreements that contain appropriate written assurances against unauthorized reexports before TSR may be used. In other cases, a license is required. BIS will generally grant fairly broad licenses where needed to cover deemed exports to non-U.S. engineers working legitimately in U.S. companies.

License applications under the deemed export rule require firms to provide detailed information on the foreign national's name, place of birth, where he or she grew up, and current location. Firms must provide a clear explanation of the type of work that will be done and the technology and source code to which the foreign national will have access. Applications must indicate whether the foreign national will work in the U.S. or abroad, and whether he or she will

 bflowe@bcr-dc.com

travel outside the U.S. BIS also requires companies to state whether they plan to sponsor those employees for permanent residency or expect them to leave the U.S. after their term of employment. Often, the approved license will apply only to the job description provided, requiring companies to apply for new licenses whenever the employee's job functions change.

Thus, part of the art of the application process is to define the employee's job description as broadly as possible to preserve flexibility, while giving the government licensing officers enough specificity to know what they are licensing and that the employee will not have access to unauthorized technology or source code. Nevertheless, BIS and other agencies have been scrutinizing deemed export applications even more than other licenses, and timelines are longer. In general, they expect applications to provide more details than before about proposed foreign national recipients (e.g., need to explain even small time-gaps in applicants' employment records and provide at least abstracts of articles written by them).

Companies proposing to release technology or source code to foreign nationals working on time-sensitive projects should be aware that processing delays may jeopardize corporate plans. In Fiscal Year 2011, BIS advised that foreign national license applications were averaging about 36 calendar days to process. Applications involving any controversial issues (e.g., access of PRC national to "sensitive" technology, or applications involving Country Group E nationals) might take more than 6 months to process, and approval is not guaranteed. BIS makes available on its web site (www.bis.doc.gov/deemedexports/) guidance on how to prepare foreign national license applications and also other guidance concerning the deemed export rule.

7. Controls on Encryption Products and Technology.

Export controls on products with encryption functions, no matter how small a part of an item, remain some of the most complex and difficult in the EAR despite many liberalizations since 1996. That is in part because Note 1 to Commerce Control List ("CCL") Category 5, Part 2 (Information Security), states:

> The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components, or functions is determined in Category 5, part 2 even if they are components or "electronic assemblies" of other equipment.

The complexity is also a vestige of many years of changes to export controls on products with cryptographic functions. Jurisdiction over cryptography was transferred to the Commerce Department, under the controls of the EAR, in December 1996. Since that time, there have been many policy revisions and even more proposals for revisions, on an almost annual basis, which keeps the regulations ever-changing and complex.

This section summarizes the most recent revisions, explains the structure of the EAR applicable to encryption items, and then walks you through a way to analyze products containing encryption functions from the least restrictive through the most restrictive controls.

7.1. June 25, 2010 Encryption Review and Reporting Streamlining and Ancillary "Note 4" Implementation. A lengthy interim final rule, 75 *Fed. Reg.* 36481-36503 (June 25, 2010) implements the Obama Administration's March 11, 2010 promise to replace:

 bflowe@bcr-dc.com

(1.1) the prior product-by-product classification requirements (that had a 30-day wait) for most Mass Market and most License Exception ENC-Unrestricted ("ENC-U") items, and

(1.2) the semiannual export sales reporting requirements for most ENC-U products with

(2.1) an annual registration of companies producing encryption items, and

(2.2) an annual end of year report of encryption products developed or exported over the year.

The rule also implements Note 4 to CCL Category 5, Part 2, which decontrols items that had been previously referred to as "ancillary cryptography" (items other than those using encryption for the principal purpose of computing, communications, networking, or information security purpose where the cryptographic functions are limited to the specific functions of the item). This change replaces the two flavor "ancillary crypto rule" (ENC-U version and Mass Market version) with one rule that allows self-classification decontrol out of Category 5, Part 2 of all qualifying products.

A rule implemented in January 2011, described below, removes from EAR jurisdiction all qualifying Mass Market and License Exception TSU encryption software that is "published" (available without charge or other restriction other than IP protection).

While the June 25, 2010 rule did not provide most of the encryption reform changes for which industry had been clamoring during the past decade, the Administration has promised that this was the first step and that BIS is seriously working with exporters to truly streamline and clarify the current cumbersome and overly complex encryption controls.

Industry has long been asking to eliminate restrictions on open cryptographic interfaces for Mass Market and ENC-U items that do not apply to open source products or in other countries; to allow chips, ASICs, software and other components specially designed for Mass Market items to be classified as Mass Market; to remove vestiges of the ITAR from the EAR, to eliminate all reporting requirements; to eliminate all reviews for Mass Market and ENC-U products, to create a positive list of what is controlled as opposed to the current broad list with about seven ways to qualify items for export without a license to all but five countries, to eliminate controls on all publicly available software, and to increase License Exception ENC-Restricted ("ENC-R") thresholds such as encryption throughput based on foreign availability. Current "controls" on products with encryption functions are more of an information gathering tool for the U.S. Government than a restriction on exports, and export controls are not well suited for that job. TechAmerica and other trade associations submitted detailed comments on the rule, focusing mostly on what more was needed, including a proposed new outline of encryption controls.

7.1.1. Overview of Review and Reporting Streamlining for Most ENC-U and Mass Market Products. This change moves exporters closer to the full standard of self-classification for items with encryption functions that is the norm for non-crypto products, but does not get fully there yet. The rule requires a more streamlined report of most Mass Market and ENC-U products at the end of the year that will take some getting used to, including the fact that most such items will not require a BIS classification CCATS number anymore. ("CCATS" are formal BIS classifications.) The good news is that exporters do not need to hold up new product distribution awaiting filing and review of applicable encryption classifications, the

classification reporting will be less onerous than CCATS applications, and there should be less need for second guessing by BIS/National Security Agency ("NSA") of whether most products are classified 5X992 Mass Market with no reporting versus 5X002 ENC-U with no reporting, as there is no substantive difference between the two (neither requires reporting of shipments unless the product does not qualify for streamlined treatment). According to BIS, the streamlined procedures should apply to between 70-85% of all products for which they have received classification requests in the past.

The rule does add new complexities in that License Exception ENC (EAR 740.17) now comes in more flavors:

> (a)(1) for exports without review to private sector developers headquartered in Supplement 3 countries for internal development end-use, without review (no change).
>
> (a)(2) for exports to "U.S. subsidiaries" for any internal end-use without review (no change).
>
> (b)(1) [Mainly New, the streamlined ENC-U] for exports of any items not covered by (b)(2) (mostly unchanged) or (b)(3) (now a subset of the old (b)(3) described below) immediately after company registration with BIS and receipt of an Encryption Registration Number ("ERN") via SNAP-R filing, with end of year reporting of self-classification of all such products in spreadsheet format with some details on encryption functions, but not usually Supplement 6 level details (unless requested).
>
> (b)(2) for items such as network infrastructure based on mostly unchanged technical parameters, source code, and others as specified, but now also including items with penetrating capabilities that are capable of attacking, denying, disrupting, or otherwise impairing the use of cyber infrastructure or networks (existing classifications are grandfathered), requiring the same full encryption classification application and approval and semiannual sales reports as before.
>
> (b)(3) [Revised] for the portion of the former ENC-U products (not described in (b)(2)) that still require (as before this rule) full encryption classification applications, a 30-day wait prior to export, and semiannual shipment reporting for:
>
> > (i) specified components and related or equivalent software – (A) chips, chipsets, electronic assemblies, and field programmable logic devices; (B) cryptographic libraries, modules, development kits, and toolkits, including for operating systems and cryptographic service providers; (C) application specific hardware or software development kits implementing cryptography;
> >
> > (ii) encryption commodities, software, and components that provide or perform "non-standard cryptography" as defined in EAR § 772 (*e.g.*, China's WAPI and other nonpublished proprietary crypto not recognized by standards bodies);
> >
> > (iii) encryption commodities and software that provide or perform vulnerability analysis, network forensics, or computer forensics functions as further described in the regulation;

 bflowe@bcr-dc.com

(iv) Cryptographic enabling commodities and software. Commodities and software and components that activate or enable cryptographic functionality in encryption products which would otherwise remain disabled, where the product or cryptographic functionality is not otherwise described in paragraphs (b)(2) or (b)(3)(i).

(b)(4) same exclusions from classification request, registration, and reporting of self-classification for crypto limited to short range wireless not controlled by CCL Category 5 otherwise; reexports of non-U.S. products developed with or incorporating U.S.-origin encryption source code, components, or toolkits (though such products need reviews before being exported from the United States). (Former "ancillary crypto" provisions deleted that have been subsumed by new Note 4, described below.)

The Mass Market provisions of EAR § 742.15 are similarly broken down into (b)(1) items that may be exported immediately after receipt of an ERN. Items described in (b)(3) (essentially the same as 740.17(b)(3) above, except for (iii), which are no longer eligible for Mass Market treatment) still require full classification request submission and a 30-day wait. Items described in 740.17(b)(2) still do not qualify in the United States for Mass Market treatment, even if they meet the Mass Market criteria. Now, items that perform vulnerability analysis, network forensics, or computer forensics do not qualify either.

Technology is also now allowed for export under ENC-R after full review to non-government end-users in destinations other than Country Groups D:1 or E:1 other than for cryptanalytic items, non-standard cryptography, or open cryptographic interfaces. Publicly available encryption technology has not been subject to the EAR since 1996, unlike publicly available encryption software. BIS did not change License Exception TSU provisions for open source and object code software, which are still eligible for export after an e-mail notification.

Exporters can still seek formal classifications via a CCATS request for any product, just as with other ECCNs. Exporters just are no longer required to do so for the new Section 740.17(b)(1) or 742.17(b)(1) items. Such optional classification requests can be reviewed by BIS without review by other agencies. Exporters also no longer need to make a separate submission for required classifications to the ENC Request Coordinator at NSA; BIS will coordinate NSA's review by forwarding submissions when required as it does for license review by other agencies, a long overdue development.

To take advantage of the new "self-classification" provisions, exporters need to submit an encryption registration of the company and types of encryption products it exports and obtain an Encryption Registration Number, and report annually its self classifications, as described further below.

7.1.2. <u>Ancillary Note 4 Implementation</u>. In October 2008, BIS amended the EAR to allow self-classification of Mass Market items under ECCN 5X992, and other items under 5X002 ENC-U, if their cryptographic functionality was specifically limited and ancillary to the limited purpose of such products (*e.g.*, LCD TVs, games and gaming, etc.). The United States sought and persuaded Wassenaar members to decontrol such products altogether at the Wassenaar Plenary meeting in 2009, and this is implemented via Note 4 to CCL Category 5, Part 2. Accordingly, exporters can now self-classify out of Category 5, Part 2 products that (a) are not primarily computing, sending, receiving, or storing information (question whether this excludes

database software), networking, or information security if (b) the cryptographic functionality is limited to supporting their other primary functions. Rather than being decontrolled to 5X002/ENC-U or 5X992 as in the past, such items will be removed from Category 5, Part 2 of the CCL altogether, even if they have other limited decontrolled cryptography, such as authentication, access control, or password protection. Exporters need to review the rest of the CCL to determine what ECCNs apply. If no other ECCN applies, the classification drops to the basket category EAR99.

The preamble of the June 25, 2010 rule included the prior examples of qualifying products that met the former definition of "ancillary" in EAR Part 772 and BIS presentations.[2] We think these examples should be included in the EAR itself, either in a new commodity interpretation (EAR Part 770) or in the Supplement 3 to EAR Part 774, Statement of Understanding, which addresses Note 4. BIS has promised at least to make them available on its website. The term "ancillary" has been dropped. Items formerly self-classified or classified by BIS as "ancillary" following the October 3, 2008 rule are grandfathered into Note 4 eligibility and are no longer classified under Category 5, Part 2. As previously and with other ECCNs, exporters can seek a formal BIS classification to confirm Note 4 eligiblity, but are not required to do so.

7.1.3. Benefits and Drawbacks of the Streamlining Rule. For most ENC-U and Mass Market items, exporters can do a simple export registration, self-classify products throughout the year, and submit a report on the self-classifications at the end of the year. The

---

[2] The list includes:

- Piracy and theft prevention for software or music;
- games and gaming
- household utilities and appliances
- printing, reproduction, imaging and video recording or playback (not videoconferencing)
- automation (e.g., supply chain management, inventory, scheduling and delivery)
- industrial, manufacturing or mechanical systems (e.g., robotics, heavy equipment, facilities systems such as fire alarm, HVAC)
- automotive, aviation, and other transportation systems
- business process modeling
- LCD TV, Blu-ray / DVD, video on demand (VoD), cinema, digital video recorders (DVRs) / personal video recorders (PVRs) – devices, on-line media guides, commercial content integrity and protection, HDMI and other component interfaces
- Medical / clinical – including diagnostic applications, patient scheduling, and medical data records confidentiality
- Academic instruction and testing / on-line training - tools and software
- Applied geosciences – mining / drilling, atmospheric sampling / weather monitoring, mapping / surveying, dams / hydrology
- Scientific visualization / simulation / co-simulation (excluding such tools for computing, networking, cryptanalysis, etc.)
- Data synthesis tools for social, economic, and political sciences (e.g., economic, population, global climate change, public opinion polling, etc. forecasting and modeling)
- Software and hardware design IP protection (note: extension of existing electronic design automation (EDA) exclusion in 5.A.2. Decontrol Note c.4 to products beyond integrated circuits and semiconductor devices, where the products are not otherwise cryptographic / cryptanalytic in nature)
- Computer aided design (CAD) software and other drafting tools

 bflowe@bcr-dc.com

changes take some getting used to, but removal of reporting for most ENC-U sales and streamlining of product submissions for most Mass Market and ENC-U products are welcome improvements. The ability to get technologies approved under License exception ENC beyond just "U.S. subsidiaries" is also a welcome improvement. While exporters can export such technologies to Country Group B destinations (the inverse of D:1 and E:1), distribution of ENC-R commodities and software is still limited to the Supplement 3 countries (*i.e.*, Favorable Treatment Countries ("FTCs")[3]) and non-government entities in other than E:1 and FTC, another tradeoff of additional complexity for slight liberalization.

Unfortunately, as described above, the June 25, 2010 changes did nothing to make the rules less complicated, other than reducing the categories of ancillary products from two to one. In fact, they are more complex than before (the rule was 22 pages of *Federal Register* fine-print), and will remain the most confusing part of the EAR for most exporters and most regulatory officials. The Orwellian split making some products "more Mass Market than others" is particularly unfortunate, given that most allies can self-classify any product that meets the "crypto Mass Market note". It also does not help exporters of ENC-R products, chip and ASIC makers (other than eliminating most reporting), and software with open cryptographic interfaces, among others. So, statements by BIS officials and others that this was only the first step towards encryption reform are particularly welcome.

Exporters can self-classify to an extent, but do remember that in a strict liability regime, one must still be accurate when self-classifying. So, when self-classifying, be sure to check facts carefully, document the classification rationale, and use these revised regulations to improve compliance. Otherwise, obtain formal CCATS classifications, either as usual or with the full Mass Market, ENC-U, or ENC-R classifications. Exporters should continue to press for reform.

7.2. Structure of Revised Encryption Controls.

Encryption controls are set forth principally in the following sections of the EAR:

Part 774, Supplement 1, CCL, Category 5, Part 2 covers information security items. ECCNs 5A002, 5B002, 5D002, and 5E002 control encryption hardware, test/inspection/production equipment, software, and technology, respectively. Such items require a license or eligibility for License Exceptions ENC or TSU (or other License Exceptions based on situation such as TMP or BAG) to be exported to all destinations other than Canada. The basic categories are broadly written to cover most encryption algorithms using "strong" encryption, but there are numerous specific exclusions for items based on the function of the item, or how the encryption is used. Excluded items are set out in Notes at the beginning of the category and in a "related controls" section.

Items that are "decontrolled" generally move to ECCNs 5A992, 5D992, and 5E992, which allow exports under No License Required ("NLR") to all countries except embargoed countries. Some items employing encryption are excluded from control because their primary

[3] FTC Countries are: Austria, Australia, Belgium, Bulgaria, Canada, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. Supplement 3 to EAR Part 740 (2010).

 bflowe@bcr-dc.com

function is not for information security, and can be controlled under other ECCNs, or even be EAR99 items.

Section 742.15 sets out the roadmap for decontrolled Mass Market and non-Mass Market encryption items, License Exception availability, self-classification eligibility, company encryption registration requirements, and licensing policies. Key instructions are also found in the Supplements to Part 742: Supplement 5 for encryption registration, Supplement 6 for information required for mandatory classification requests, and Supplement 8 for self-classification reports.

Section 740.17 covers License Exception ENC, the primary License Exception (discussed below) for exporting 5X002 items. Some provisions of License Exception ENC are available without the exporter notifying BIS. Other provisions cannot be used unless the exporter (or manufacturer of the item) has obtained an Encryption Registration Number and submits an annual report describing the items classified. For exports of more sensitive items, submission of a CCATS classification request and a 30-day wait for a response from BIS is required. Such items are also subject to semi-annual reporting disclosing the details of actual exports.

Section 740.13 covers License Exception TSU, the authority for exports of 5D002 "open source" and "community source" code encryption as well as object code compiled therefrom.

Part 740 covers other License Exceptions such as TMP and BAG, authorizing exports of strong encryption for temporary exports (*e.g.*, beta testing) and as part of baggage on laptop computers and according to other specific terms, as applicable (many License Exceptions specifically exclude Encryption Items).

Section 734.4 sets forth special rules relating to the eligibility of encryption items for the *de minimis* provisions of the EAR, as well as differential treatment of publicly available encryption source and object code under the EAR.

Section 734.2(b)(9) has a special definition of "export" for 5X002 Encryption Items, with safe harbor provisions allowing posting of ENC-R items to Web sites and similarly making them available for export if exporters follow certain specified steps; note there is no deemed export rule for encryption technology (as a result of First Amendment litigation).

Part 772 sets forth important definitions including "Non-Standard Cryptography", "Government End-User", "Encryption Component", "Symmetric Algorithm", "Asymmetric Algorithm", "Banks", "Financial Institutions", "Business Unit", "Cryptanalytic Items", "Hold Without Action","Open Cryptographic Interface," and "U.S. Subsidiary."

7.3. How to Apply Export Control Categories for Encryption Products.

Because the revised BIS encryption regulations remain wonderfully complex, it is most useful to list the principal categories for export control treatment of different types of encryption products, beginning with the least restrictive controls and moving to the most restrictive. Exporters of encryption products should take the following steps to determine how encryption controls apply to particular products:

7.3.1. Determine Whether the Encryption Is Eligible for the Medical Note.

 bflowe@bcr-dc.com

N.B. to Note 1 to Category 5, Part 2 provides that "[c]ommodities and software specially designed for medical end-use that incorporate an item in Category 5, part 2 are not classified in any ECCN in Category 5, part 2." Thus, if your end-item is specially designed for medical end-use and has or calls cryptography, it is self-classifiable under a non-encryption classification. Note that the encryption itself does not need to be restricted to a medical function, but rather it is the functionality of the end-item that determines eligibility. Exporters would still need to review the rest of the CCL to determine which ECCN, if any, applies; however, almost all items specially designed for medical end-use are classified as EAR99 by the "Medical Note" in Supplement 3 to EAR 774.

7.3.2. Determine Whether the Encryption Is Eligible for Note 4 to CCL Category 5, Part 2 (formerly "Ancillary"). As discussed above, items that use encryption but whose primary function is not computing, networking, communications (sending, receiving, or storing information), or information security are excluded from control under Category 5, Part 2. As noted above, the July 25, 2010 *Federal Register* notice also includes a list of examples of types of products that qualify for Note 4 (*e.g.*, LCD TVs, games and gaming, and many other examples, most of which previously were in the EAR definition of "ancillary"). (*See* 75 *Fed. Reg.* 36482, 36488.) Note 4 eligibility is driven by the product's primary functionality, not the way encryption is used. Exporters can self-determine Note 4 eligibility or can seek a formal classification from BIS. Items that were self-classified or classified by BIS as "Ancillary" items (whether 5X002 ENC-U or 5X992 Mass Market) between October 3, 2008 and June 25, 2010 are grandfathered as eligible for Note 4.

Items that use cryptography solely for intellectual property and copy protection/license management are eligible for Note 4. Such items were formerly decontrolled to 5D992 under 5A002 Related Controls notes.

An additional consideration when applying Note 4 is that BIS has indicated, without much elaboration, that encryption components not incorporated into the end-item and related encryption technology may not qualify for the exemption.

7.3.3. Determine Whether Encryption Is Eligible for Self-Classification Under ECCNs 5A992, 5D992, or 5E992 (Without Notification or Review). Encryption items are self-classifiable as 5A992/5D992/ 5E992 (collectively "5X992) if they are so-called "weak" encryption items that use only 56-bit or less symmetric, 512-bit asymmetric or less, or 112-bit or less elliptic curve cryptographic items. In addition, Mass Market items using only up to 64-bit symmetric algorithms are self-classifiable as 5X992. *See* EAR § 742.15(b).

The current controls also permit self-classification of Mass Market items as 5X992 if the items qualify under exemptions for "short range wireless" without prior review or encryption registration (such items are also exempt from ENC prior review requirements, discussed below.)

Items that are specifically excluded from control under 5A002 or that have limited cryptographic functionality have long been eligible for self-classification under 5X992. The types of items that are excluded or considered to have limited cryptographic functionality are listed in at the "Related Control Notes" to ECCN 5A002, as well as in the ECCN 5A002.a.1 and its following Technical Note. Examples of exempt items eligible for self-classification under 5X992 are those where cryptographic functionality is limited to digital signature, authentication,

fixed coding or compression techniques, personalized smart cards, money or banking functions, and telephone handsets not capable of end-to-end encryption.

Examine carefully the specific provisions of these exemptions to determine whether the item qualifies. To qualify, all cryptographic functions must fall under an exempt category. If the 5X992 decontrol classification is ambiguous, consider a formal BIS classification.

In some cases, items may be eligible for self-classification as EAR99 items. Data, music, and other information with only copy protection controls and items subject to the Medical Note to the CCL. *See* EAR § 774, Supplement 3 and Note 4 to EAR § 774, Category 5, Part 2.

Note: Even if a product is not subject to controls for Encryption Item ("EI") reasons, an exporter must also ensure that it is not subject to export controls under another ECCN. The most restrictive ECCN applicable to a product governs, which is why encryption controls are a principal concern, but they are not the only export controls that may apply. Note 1 to Category 5, Part 2 treats items as subject to encryption controls if they have any encryption function regardless of whether they are incorporated into something else, but BIS in practice does tend to apply the strictest classifications even if the EAR does not specify that this should be done.

7.3.4. Non-U.S. Product Incorporating U.S. Encryption. Non-U.S. products that incorporate U.S.-origin encryption components qualified for export can themselves qualify for reexport under License Exception ENC without prior review or ERN. This includes non-U.S.-made items that call on U.S.-origin cryptographic interfaces or libraries. However, such items are subject to any applicable encryption registration or prior review requirements if they are going to be exported from the United States. So, most non-U.S. companies that want to sell their products worldwide eventually qualify them specifically under the EAR so their customers can export them easily. Applications should make clear if they otherwise are not subject to the EAR.

7.3.5. Mass Market Items Requiring Review or ERN. Mass Market items not mentioned previously require either that the exporter or manufacturer obtain an ERN or file a review request.

The Mass Market criteria are set forth by the Cryptography Note. Eligible items must meet all of the following:

(a) generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following: (i) over-the-counter transactions, (ii) mail order transactions, (iii) electronic transactions, or (iv) telephone call transactions;

(b) cryptographic functionality cannot be easily changed by the user;

(c) designed for installation by the user without further substantial support by the supplier; and

(d) when necessary, details of the items are accessible and will be provided, upon request, to BIS and/or NSA in order to ascertain compliance with these

 bflowe@bcr-dc.com

conditions.

This is the last point where the United States differs from allies in requiring classification requests or now ERNs, as follows.

EAR 742.15(b)(6) lists the following examples of Mass Market encryption products:

> [G]eneral purpose operating systems and desktop applications (*e.g.* e-mail, browsers, games, word processing, database, financial applications or utilities) designed for, bundled with, or pre-loaded on single CPU computers, laptops, or hand-held devices; commodities and software for client Internet appliances and client wireless LAN devices; home use networking commodities and software (*e.g.* personal firewalls, cable modems for personal computers, and consumer set top boxes); portable or mobile civil telecommunications commodities and software (*e.g.* personal data assistants (PDAs), radios, or cellular products); and commodities and software exported via free or anonymous downloads.

This list is illustrative, not comprehensive.

Items listed in EAR 742.15(b)(3) are not eligible for classification and export as 5X992 NLR unless the exporter has filed a classification request with BIS and waits 30 days. Such items include chipsets, encryption components, encryption toolkits, items that use non-standard cryptography, and items that provide or perform vulnerability analysis, network forensics, or computer forensics functions. Upon filing of the Encryption Registration request described below, other Mass Market items are eligible for export as 5X002 ENC-U items to the FTCs and subsidiaries of companies headquartered in FTCs.

All other Mass Market items are eligible for self-classification as 5D992 Mass Market if the exporter or manufacturer has obtained an ERN, as described below. Note that an exporter who is exporting a vendor-supplied Mass Market item may rely on an ERN issued to the manufacturer that covers the manufacturer's item.

EAR 740.17(b)(2) items are not eligible for Mass Market treatment even if they otherwise meet the criteria. BIS also has long taken the position that semiconductor devices and application specific integrated circuits do not qualify as Mass Market encryption items even if sold in large quantities if they are not sold directly to the general public, but we advise applicants to challenge that notion for items used only for Mass Market end-items. Getting a Mass Market classification from another Wassenaar Member country can help given that products would otherwise be classified under different ECCNs (5X002 in the United States and no ECCN elsewhere) by different Member countries.

7.3.6. <u>5X002 Items – Exports to U.S./FTC Subsidiaries</u>. 5X002 items can be exported under License Exception ENC without obtaining an ERN or filing a classification request if (a) they are for the internal use of a non-U.S. affiliate of a U.S. company that qualifies as a "U.S. subsidiary" (except in embargoed countries); or (b) they are for internal use for the development of new products by a company headquartered in the FTCs, or their subsidiaries (except in embargoed countries). These exemptions also permit release to non-U.S. national employees, independent contractors, and interns employed by such companies.

 bflowe@bcr-dc.com

7.3.7. 5D002 Items - Publicly Available Source and Object Code. Open source code and compiled object code from it that is free would normally be exempt from the EAR as publicly available items. However, if they contain cryptographic functionality, BIS deems them subject to EAR jurisdiction. Nevertheless, such items are eligible for export under License Exception TSU, provided that the URL location of the source code or object code has been e-mailed to BIS and NSA. However, TSU does not apply to other object code "freeware" compiled from other sources. TSU also does not authorize exports of proprietary software containing only open source encryption components such as OpenSSL, which often surprises exporters. If the item qualifies for TSU, the exporter need not provide updates if it elects to provide the Internet location rather than providing disks. Section 740.13(e) purports to restrict knowingly exporting to the embargoed countries (which are not restricted from receiving publicly available products), but provide that posting to the Web is not "knowledge" and does not trigger red flags. (*See also* discussion in Part 13 below on the new Treasury Department General Licenses for free and anonymous software exports to embargoed countries and BIS's new rule on same.)

7.3.8. 5X002 Items Not Listed in Section 740.17(b)(2) or (b)(3) qualify for (b)(1). 5X002 items other than those listed in Section 740.17(b)(2) or (b)(3) can be self-classified and determined to be eligible for ENC-U if the exporter or manufacturer has obtained an ERN and complies with the annual self-classified product report requirement. EAR 740.17(b)(1). Note that, while denominated a "self-classification" report, BIS has advised that (b)(1) items voluntarily submitted for a formal BIS classification must be included in the annual report, as well. Once qualified, they may be exported and reexported under ENC-U to any end-user, except to embargoed countries.

7.3.9. 5X002 Items – Sections 740.17(b)(2) and (b)(3) Items. Items listed in Sections 740.17(b)(2) (ENC-R) and 740.17(b)(3) (ENC-U) remain subject to a required commodity classification request and 30-day wait. Export is generally permitted to FTCs and FTC-headquartered companies once a classification request has been filed. Certain ENC-R items, particularly cryptanalytic items, are also subject to distribution restrictions to government end-users within the FTC. ENC-R items may be exported to any end-user in or headquartered in any of the FTC destinations, and to any non-government end-user outside the FTC destinations, but require a license to government end-users outside the FTC destinations. EAR Part 772 defines the term "government end-users," which does not include some types of government agencies and many types of government-owned companies. ENC-U items under (b)(3) may be exported to all end-users in all but E:1 countries.

7.3.10. 5X002 Items – ENC Ineligible – License Required. A few items and situations are not eligible for License Exception ENC use, and a license is required:

1. Prior Review Requirements Not Met for ENC-R and Section 740.17(b)(3) items.
2. Cryptanalytic Items to Government end-users
3. Open Cryptographic Interface to Non-FTC & Non-FTC subsidiaries
4. Exports to E:1 Countries (Cuba, Iran, North Korea, Sudan, Syria)
5. Source Code or Technology to E:1 Nationals

7.3.11. Mechanics of Revised Encryption Structure. We summarize below the key requirements, but it is worthwhile to review the extensive BIS guidance at: http://www.bis.doc.gov/encryption/default.htm.

7.3.11.1. Obtaining an Encryption Registration Number ("ERN"). Obtaining an ERN is a prerequisite to self-classification of eligible ENC-U items under Section 740.17(b)(1) or Mass Market under Section 742.15(b)(1). An ERN is also required for filing a required classification request. The process of obtaining an ERN is fairly simple. SNAP-R (BIS's online application system) has a new form used to obtain an ERN. SNAP-R users with first-party filing rights can file for their own ERN. Third-party filers can also obtain an ERN for clients (SNAP-R registration for the client is not required).

The SNAP-R form is fairly simple. The applicant's contact information is provided along with very basic information about their encryption products by completing Supplement 5 to Part 742 and uploading into SNAP-R. An ERN is issued through SNAP-R immediately. Parent companies can file to cover their subsidiaries and affiliates, as long as the information provided covers all the affiliates' products.

Obtaining a replacement ERN is required only if the information originally submitted changes. One can update that information as soon as it is changed, or wait until the end of the year. ERNs are issued serially, so instead of retaining the same number, a new ERN will be issued when the information is updated.

7.3.11.2. Annual "Self-Classification" Report. As noted above, the other prerequisite to self-classification and eligibility for ENC under Section 740.17(b)(1) or Mass Market under Section 742.15(b)(1) is submission of an annual report advising BIS (and NSA through BIS) what items have been self-classified during the year. Reports are due on February 1st for the previous year. The information required is found in Supplement 8 to Part 742, and is much more general than the Supplement 6 information required for a mandatory classification request. The reports must be submitted electronically in comma-separated value (.csv) format. One counterintuitive aspect of this requirement is that, despite being called "self-classification" reports, BIS has advised that Section 740.17(b)(1)/742.15(b)(1) items submitted for voluntary formal classifications must be included in the report. BIS indicated that the reason for this is to be able to provide NSA with a complete database of (b)(1) eligible items. Unlike Sections 740.17(b)(2) and (b)(3)/742.15(b)(3) items, which are referred to NSA for classification assistance, only BIS will review classification requests for Sections 740.17(b)(1) and 742.15(b)(1) items.

7.3.11.3. Clarification of Information Required for Encryption Classifications. While EAR § 748.3(d) still indicates that the information in Supplement 6 to Part 742 is required for encryption classifications, EAR § 740.17(d) clarifies that Supplement 6 information must be submitted only for mandatory classification requests for Sections 740.17(b)(2), 740.17(b)(3) and 742.15(b)(3) items. For optional classification requests, only information sufficient to allow BIS to confirm the item is not classified under Sections 740.17(b)(2), 740.17(b)(3) or 742.15(b)(3) is required. The SNAP-R form now has a check box that says "Check here if you are submitting information about encryption required by Section 740.17 or 742.15 of the EAR." Checking that box creates three drop-down options in SNAP-R: "License Exception ENC," "Mass Market Encryption," and "Encryption - Other." The first option should be selected for Sections 740.17(b)(2) and 740.17(b)(3) items, the second for Section 742.15(b)(3), and the third option for any other encryption items submitted for review.

7.3.11.4. Further Tips for Applications. Exporters seeking ENC-U treatment should explain why their product does not meet any of the ENC-R listed criteria.

 bflowe@bcr-dc.com

Within 30 days of a properly submitted required review request, exporters may assume that their product qualifies under the applicable provisions. We still prefer to obtain a positive answer. BIS can stop the clock by asking questions and holding the case without action, and such days do not apply to the 30 day time period.

Applicants do not need to request for the *de minimis* rule to apply. EAR § 734.4 specifies which encryption items automatically qualify for *de minimis* eligibility and under what criteria. Exporters of software should be aware that further review under the provisions of EAR § 734.4 will be required for non-U.S. items incorporating such products to qualify for exemption from the EAR under *de minimis* rules.

7.3.11.5. Semi-Annual Shipment Reporting Requirements for License Exception ENC Exports. EAR § 740.17(e) sets forth reporting requirements for exports under License Exception ENC. Under the revised structure, semi-annual reporting of exports is required only for Section 740.17(b)(2) ENC-R items and Section 740.17(b)(3)(iii) items. Reporting requirements apply only to exports from the United States and to reexports from Canada. Thus, exporters who ship to distributors overseas need only report their exports to those distributors, and need not collect information on further sales in the distribution chain. However, if end-user name and address information for distributor sales is "collected in the normal course of business," the exporter must report the end-user's name and address. Thus, exporters must report information collected on warranty registration cards if collected from end-users in the normal course of business. But, the term "collected as part of the distribution process" was used so as not to require reporting of odd data obtained here and there by individual employees, such as a salesman overseas, for example.

Short range wireless, client Internet appliances, client wireless LAN cards, ENC-U general purpose operating systems or desktop applications such as browsers, e-mail, word processing, database, games, financial applications or utilities), 64-bit symmetric items, and reexports (other than from Canada) have long been exempt from reporting requirements. The October 3, 2008 revisions to the regulations added exemptions for personal area networking items and ancillary cryptography items. Most of these exemptions remain in the EAR, but were essentially mooted by the June 25, 2010 rule, as most such items are either no longer classified under 5X002 pursuant to Note 4 and/or are exempt from reporting under EAR § 740.17(b)(1).

The EAR had seemed to invite exporters to request further reporting relief in specific applications if they could provide adequate justification, though BIS has only granted such relief via interpretations of the regulatory provisions, rather than creating new exemptions. The October 3, 2008, revisions to License Exception ENC added an explicit option for BIS to grant *ad hoc* exemptions from reporting requirements to items, and we have obtained such exemptions for certain clients for products the reporting of which apparently is not needed by BIS/NSA. However, the June 25, 2010 rule eliminated the provision for asking for and obtaining a product specific reporting exemption. BIS officials says they will still consider such requests.

7.3.11.6. License Exception ENC Eligibility (After Registration of Review Request) for Exports to Any End-User in FTC. The Notes to Sections 740.17(b)(2) and (b)(3) authorize exports of any encryption items under License Exception ENC regardless of key length to any end-user located in the FTCs, and to non-U.S. subsidiaries or offices of firms, organizations, and governments headquartered in an FTC wherever located (other than in embargoed countries). Exporters must submit an application first (for Section 740.17(b)(2)

ENC-R and Section 740.13(b)(3) items), but then may immediately make such exports. Again, exports for internal development of new products by private sector companies located in the FTC and their subsidiaries do not require registration of a review request pursuant to EAR § 740.17(a)(1).

7.3.11.7. License Exception ENC Compliance Tips. Exporters need to take appropriate steps to make sure that they do not ship ENC-R items to governments outside the FTC, and that their distributors and resellers understand that they may not export, reexport, or even transfer within non-U.S. countries to governments any ENC-R products or those otherwise eligible for such export. We recommend obtaining certifications from distributors and end-users with respect to such exports.

Section 734.2(b)(9)(iii) provides clear guidelines on the limits of what is required for posting ENC-R encryption products under this provision on the Internet, with warnings as to "Know Your Customer Guidelines" and avoiding violating the other EAR General Prohibitions against illegal exports. Many follow this model for other products. For active electronic shipments (*e.g.*, e-mails) or actual exports, we recommend having shipping personnel document screening by use of at least a simple export compliance checklist.

7.3.11.8. Commercial Source Code That Is Not Publicly Available. EAR § 740.17(b)(2) provides that proprietary encryption source code not publicly available pursuant to EAR § 740.13(e) (License Exception TSU) will qualify as ENC-R, and thus requires prior review and classification and may not be exported to governments outside the FTC. It may be exported to anyone in the FTC and to non-government end-users in countries outside the FTC. It is eligible for immediate export to non-government entities upon registration of the review request. Providing a copy of the source code with the review request is no longer required. Such code is subject to the reporting requirements under the same criteria as other ENC exports.

7.3.11.9. Open Cryptographic Interfaces. Items incorporating an Open Cryptographic Interface may be exported under License Exception ENC-R to any end-user in the FTC (after registration of a completed review request) pursuant to 740.17(b)(2)(iii) or to U.S. subsidiaries for internal use, or to FTC headquartered private sector end-users and their subsidiaries for internal research and development use, but otherwise require a license. In contrast, Open Cryptographic Interfaces in open source products may be exported under License Exception TSU without restriction after the TSU notification is submitted. This is a very controversial limitation that software companies are seeking to eliminate given the competitive advantage it gives to open source products. BIS is reportedly approving some Encryption Licensing Arrangements for products with Open Cryptographic Interfaces, and approved Microsoft Vista for Mass Market treatment only after other countries did so.

7.3.11.10. Reexports of Resultant Non-U.S.-Produced Products and the "Crypto-Aware" Concept. Non-U.S. products developed with or incorporating U.S.-origin encryption source code of any type, components, or toolkits of any type remain subject to the EAR but do not require review and classification by BIS and can be exported or reexported without further authorization. EAR § 740.17(b)(4)(ii). Such non-U.S. items include those "designed to operate with U.S. products through a cryptographic interface." This statement clarifies that such items are exempt from review requirements, but at the same time implies they are in fact presumptively subject to *U.S. jurisdiction* without more direct inclusion of U.S.-origin products – or else why would an exemption from the prior review requirement be necessary?

 bflowe@bcr-dc.com

However, we do not think that BIS can amend the EAR to expand extraterritorial jurisdiction beyond what is set out in EAR §§ 734.3 and 736 (*i.e.*, there needs to be some U.S.-origin content or direct product of U.S.-origin National Security controlled technology for the non-U.S.-origin items to be subject to the EAR).

This seems to reflect an increasingly conservative interpretation by BIS in recent years of the applicability of License Exception ENC review requirements to items that do not themselves incorporate encryption functions algorithms in their code, but rather call out to separate products with encryption functions or to operating system elements via a cryptographic interface (*e.g.,* the Microsoft Crypto API or java) to provide security functions. Such items have been informally dubbed "crypto-aware" items by NSA/BIS, and are controlled as products designed or modified to "use" cryptography (a stricter reading of ECCN 5A002). This is usually a shock to programmers and others new to encryption controls. Whether such items are subject to prior classification requirements has been a hotly debated question over the years, with reasonable arguments made on both sides.

As a result of these discussions, BIS had agreed to permit a "crypto-aware" item to be derivatively classified under the same ECCN as the item it calls on, provided that the item being called upon had been previously reviewed by BIS (*e.g.*, Windows, Java Mass Market programs), and that the exporter made an e-mail notification setting forth a general description of the item, plus Part 742, Supplement 6 information. These were informal interpretations, though provided in public meetings. So, for example, if an item called on Windows XP through the Microsoft Cryptographic API, and had no other controlled crypto functions, it would take on Windows XP's 5D992 classification after notification.

Current BIS personnel changed this interpretation in recent statements at conferences, as well as in the context of classification reviews, where they have said instead that a "crypto-aware" product cannot be derivatively classified based on the classification of the item called upon, but rather should be classified as a new encryption item via the License Exception ENC or Mass Market review procedures. This may be a reasonable interpretation, but it nonetheless represents a rollback of prior interpretations that were also reasonable and have been relied upon. Applying this new, more expansive interpretation is much less defensible for non-U.S. products that have no actual U.S. content and thus are not subject to the EAR pursuant to Parts 734 and 736.

7.3.11. Encryption Licensing Arrangements (ELAs) and Other Licenses.

The regulations continue specifically to provide that Encryption Licensing Arrangements ("ELAs") will be favorably considered for exports to governments or Internet Service Providers and telecoms for services to governments specific to civil government end-users. Expect to see certain governments excluded upon case-by-case review. BIS curiously removed the provisions saying that ELAs are "likely to be approved" for export to strategic partners of U.S. companies (defined in Part 772), but they have continued to approve such ELAs. Exporters can seek to persuade BIS and NSA to grant ELAs to other classes of end-users whom they can define clearly, and can otherwise apply for licenses to exports to other parties (*e.g.*, military users) on a case-by-case basis. ELAs are now valid for a standard four-year term. But BIS/NSA have been placing restrictive conditions on the export and use of WAPI and possibly other nonstandard cryptography since the June 25, 2010 rule.

7.4. Concerns Remain Regarding "Hidden" Licensing Requirements for Offshore

 bflowe@bcr-dc.com

Development and Sales of Encryption Items.

One of the more difficult encryption provisions had been EAR § 744.9, which prohibited technical assistance, including training, intended to aid a non-U.S. person in the development or manufacture outside the United States of encryption software that, if of U.S. origin, would be controlled under the EI controls. Technical assistance was prohibited even if there is no licensable export (*i.e.*, even if all the information transferred in the context of the assistance is in the public domain). Section 744.9 was eliminated by BIS as part of the October 3, 2008, changes to the cryptography provisions. This provision was a leftover from the grafting of ITAR controls on encryption onto the EAR when jurisdiction was transferred in 1996, as it mirrors the concept of controlling an export of an ITAR defense service, even when all technology was decontrolled public domain technology.

Eliminating this trap for the unwary is somewhat helpful in simplifying the structure of the encryption controls, because it was something of an outlier, residing as it did amongst the various proliferation-related controls in Part 744, and because it imposed controls on activities of "U.S. persons" regardless of export, an unusual basis for control under the EAR. The EAR primarily applies to actions involving goods, technology, and software that are subject to the EAR, not to the actions of people. (N.B., Part 744.6 does contain counter-proliferation based licensing requirements applicable to the activities of U.S. persons that do not involve exports subject to the EAR.) Fortunately, BIS's Office of Export Enforcement has not enforced this provision to my knowledge, but it was difficult to advise procurement officials as to whether discussing with non-U.S. suppliers how to revise their products to meet security requirements might or might not be subject to this control.

However, it is not a major relaxation in license requirements, since removal of this provision was coupled with a warning in the License Requirements notes to ECCN 5E002, that BIS considers the provision of technical assistance that incorporates or draws upon U.S.-origin encryption technology to inherently involve the release of 5E002 technology, which would trigger licensing requirements if the technology is exported. (That is not the case for publicly available technology, which the warning does not mention.) Unfortunately, BIS did not add to this note the former provisions of EAR § 744.9 stating that no licenses were required to export technical assistance along with authorized items, so in some cases, licenses might be required when they previously were not. (Most of the time, License Exception TSU will authorize limited technical assistance exports.)

Encryption commodities and software that activate or enable cryptographic functionality in retail encryption products that would otherwise remain disabled are controlled in the same manner as the item in its activated state (assuming that the original export treated the "dormant crypto" as non-existent). This "dormant crypto rule" has been provided only obliquely in License Exception ENC and Mass Market encryption regulations, as the regulations do not expressly state the rule itself, only the corollary rule that items that activate or enable encryption functionality must be controlled as if they were the encryption functionality itself. (There is no reason to have the corollary if the dormant crypto rule were not already implicit, but it would be better if the rule was affirmatively stated.) The rule, long in unpublished BIS advisory opinions, exempts exports of software or hardware from strict "EI" controls if access control encryption functions (controlled under 5D992) prevent a user from gaining access to the crypto functions without a key; but, the exporter must restrict export of the key as if it were the crypto enabled software. Under the June 25, 2010 revision, items that enable cryptographic functionality are not, however,

 bflowe@bcr-dc.com

self-classifiable under the provisions of Section 740.17(b)(1) – even if the activated item otherwise qualifies for self-classification as ENC or Mass Market eligibility. Exporters using this rule should make sure they can secure the keys effectively, as that is often harder to do. If exporters already treated the original export as encryption controlled, then the export of the key is normally treated as only an export of uncontrolled data, though again this is not specified directly in the regulations, only by implication.

Pursuant to the 2010 Wassenaar Plenary changes to the dual use International List, a new note (j) was added to 5A002(a) to decontrol items otherwise classified under 5A002(a) if their cryptographic capability cannot be used or can only be used through "cryptographic activation." A new entry 5A002(b) was also added to control items that enable 5A002(a) cryptographic functionality. "Cryptographic activation" is defined as a secure mechanism implemented by the manufacturer, uniquely bound to the item or customer. It can be hardware, software or technology

7.5. Upgrades to Key Lengths and Subsequent Bundling.

License Exception ENC provisions, but not Mass Market, permit reporting for upgrades to encryption key lengths without having to submit a new classification request. *See* EAR § 740.17(e)(2). However, with the June 25, 2010 expansion of self-classification eligibility for ENC-U and most Mass Market items, this should create only a need to keep track of key length increases for purposes of annual self-classification reporting.

Formerly, EAR 770.2(n) provided that "subsequent bundling, patches, upgrades or releases, including name changes, may be exported or reexported under the applicable provisions of the EAR without further review as long as the functional encryption capacity of the originally reviewed product has not been modified or enhanced."

The October 3, 2008 revisions to the rules replaced EAR 770.2(n) with reworded notes, now found in Sections 740.17(d)(1)(iii) and 742.15(b)(7)(i)(C). The stated purpose was to integrate the "subsequent bundling" interpretation in the specific sections on encryption and to provide additional clarification concerning when a new encryption review is required. It makes some sense to include this interpretation as part of the core encryption provisions, but it only slightly clears up the issue of when a new review is required. The text of the revised note added language indicating that a new review is not required when there are "updates" to an encryption component that a program uses to provide cryptography (*e.g.*, Open SSL or Java components). This was very helpful, since such changes can include new algorithms or upgrades, but BIS reviews them all the time. The notes otherwise reinforce the interpretation that version changes do not require a new classification review, as long as the changes are not relevant to the product's cryptographic functionality (*i.e.*, do not affect the Supplement 6 information). This is consistent with the long standing BIS interpretation of subsequent bundling.

Despite this additional clarification, BIS has not provided clear guidance on what does and does not qualify as a change to functional encryption capacity. Clearly a change in the encryption algorithm, key exchange mechanism, or key length (unless otherwise authorized by notification) would require a new classification. BIS has also advised that a change in use of encryption from what was described in the application (*e.g.*, from storage only to communications encryption or vice versa) would require a new application. Simply coupling an already classified product on the same media as another product would not require a new

classification, but incorporating a component generally would.

7.6. Decontrol of Published Software with Encryption Functions.

After years of urging from industry, BIS finally published on January 7, 2011, a rule clearly making "not subject to the EAR" Mass Market software after it has qualified as Mass Market via either a BIS classification or self-classification, as applicable, and License Exception TSU eligible object code software compiled from License Exception TSU eligible open source (but not source code itself) if published. 76 *Fed. Reg.* 1059 (Jan. 7, 2011). Although a welcome improvement, the rule has its limitations. It did not remove all freely available "published" encryption software from being subject to the EAR, including License Exception ENC eligible software. Moreover, proprietary software incorporating or calling on publicly available software remains subject to the EAR because the item being exported does not itself qualify as publicly available. *See* revised EAR 740.13((e)(2)(i). Note also that free patches and updates that can only be used with proprietary products for customers, although one can certainly argue that point, and it appears that most patch providers do not screen their downloads in practice.

The BIS rule came in the wake of an OFAC amendment to the Sudanese Sanctions Regulations, 31 C.F.R. part 538, and the Iranian Transactions Regulations, 31 C.F.R. part 560, to add general licenses to authorize exports to Sudan and Iran of certain services and software incident to the exchange of personal communications over the Internet, such as instant messaging, chat and email, and social networking, and similarly amended the Cuban Assets Control Regulations, 31 C.F.R. part 515, to authorize by general license the exportation of such services to Cuba. (The EAR covers exports of goods, software, and technology to Cuba, as long as such services and software are publicly available at no cost to the user.) (75 *Fed. Reg.* 10997 (Mar. 10, 2010)).

That OFAC regulation was issued pursuant to a notification by the State Department to Congress that it was in the national interest to permit export of certain software and services that enable personal communications and other sharing of information over the Internet that were otherwise controlled by the CCL because of their encryption functionality. The exclusion of "published" software from the EAR by EAR 734.7 specifically did not include software classified under ECCN 5D002 or 5D992, and such software thus could not qualify as "informational materials" that otherwise would be exempt from OFAC sanctions. (EAR 734.7(c).) OFAC noted that, "[a]s events in Iran since last June's [2009] Presidential election there have shown, personal Internet-based communications are a vital tool for change." Thus, the EAR rule should allow cleaner "informational materials" treatment under OFAC rules and was a welcome improvement.

7.7. Compliance with Encryption Controls Remains Critical.

While reforms since 1996 have dramatically reduced controls over exports of encryption products, the encryption regulations remain incredibly complex. It is critical to take appropriate steps to ensure that companies do not export or facilitate exports of strong encryption products without full compliance with U.S. export controls. New enforcement cases are arising in this area every day, and the enforcement policy of the Commerce Department's Office of Export Enforcement is still evolving. Civil penalties of up to $250,000 per violation can mount up quickly with large volume exports. While it is inevitable that ENC-R encryption related products will be transferred from time to time by customers to government end-users, company personnel

must ensure that they are never responsible for such exports. Thus, steps such as labeling strong encryption products as "Requires a U.S. export license to export, reexport or transfer to many Governments," inserting appropriate clauses in license agreements or side letters and product literature, providing explicit guidance to marketing and shipping personnel as to which products cannot be exported without authorization, and similar compliance steps are critical in this area.

Also, the encryption regulations define "export of EI controlled software" to include "making such software available for transfer outside the United States over wire, cable, radio, electromagnetic, photo-optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites." This definition has the unfortunate effect of penalizing actions that people do not commonly think of as "exporting." Thus, if company personnel plan to make any EI controlled software available for downloading via websites or similar electronic distribution, they should make sure either (a) to follow the specific "safe harbor" standards of care set forth in EAR § 734.2(b)(9)(iii), or (b) apply and gain approval from BIS in writing of a different method of distribution that provides similar protections against easy access by non-U.S. nationals and persons outside the United States.

7.8. Further Changes Needed.

The Regulations and Procedures Technical Advisory Committee and trade associations have been working with BIS, NSA, and other regulators to streamline further this incredibly complex set of encryption regulations, the complexity resulting from the various changes since 1996. The main liberalizations to the once draconian encryption controls have long been accomplished, but cleaning up the controls will still take some effort.

Industry is still pushing for more fundamental streamlining, such as eliminating ECCN differences between limited-use encryption; merging License Exception TSU, 5X992 Mass Market, and ENC-U categories, so as to eliminate wasted effort distinguishing among the three categories, allowing components and toolkits designed for Mass Market items to be classified by the United States as Mass Market as other countries do, and removing more of the "virtual ITAR" control vestiges, including, as described above, treating freely available encryption software as not subject to the EAR whether or not in object code. While the October 2008 and June 2010 revisions did much to eliminate the inconvenience caused by prior review requirements for a large percentage of encryption items, U.S. industry is still burdened with complex regulations, registration, and reporting requirements. Such requirements are generally unrelated to national security export controls – *i.e.*, only with respect to a limited number of items could it reasonably be said that the U.S. Government has an interest in restricting their distribution. Thus, these provisions remain primarily a mechanism for NSA to collect information about U.S. encryption products.

As part of the overall export control reform effort the Obama Administration is undertaking, BIS has solicited input from industry about how to structure encryption export controls based on a "green field". TechAmerica and other industry groups have provided input, focusing on making U.S. controls more consistent with Wassenaar interpretations, with encryption controls driven by ECCN classification, rather than a complex structure of license exceptions and reporting requirements. *See* http://efoia.bis.doc.gov/pubcomm/records-of-comments/record_of_comments_encryption.pdf.

 bflowe@bcr-dc.com

8. Exceptions to EAR Reexport Controls.

This section discusses the application of potential exceptions to EAR reexport controls. Please see Section 6 above for guidance on the application of the primary reexport controls imposed by the EAR on which this discussion rests. In particular, even though the License Exceptions described below apply to reexports of products with U.S. content, a company should screen shipments to ensure that none of the General Prohibitions of EAR Part 736 apply. These include the list of parties denied export licensing privileges of receiving any U.S.-origin exports or reexports, parties whom the company knows will use the products in missile (now worldwide), chemical or biological weapons (now worldwide), or certain sensitive nuclear activities, and other prohibitions set forth in EAR Part 736 that apply to License Exception shipments regardless of the technical levels of the products being shipped. Only when a shipment is entirely excluded from the scope of the EAR (such as pursuant to the *de minimis* rules and public domain data) can one ignore U.S. reexport controls completely.

In order to determine whether no U.S. reexport controls apply, you will generally need to determine four things:

a. Whether all the U.S.-origin hardware products, including U.S. parts and components incorporated into non-U.S. made products, are covered by exemptions to the EAR;

b. Whether all the U.S.-origin technical data and software, and any direct products thereof, are also exempt under the EAR;

c. Whether the State Department administered International Traffic in Arms Regulations ("ITAR") apply to the products that you employ (which we do not cover here); and

d. Whether any of the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") Regulations apply to any reexports that you might make to Cuba, Iran, Sudan, any other countries subject to OFAC sanctions, or any entities or individuals on one of the Lists of Specially Designated Nationals (discussed in Section 9 below).

This section discusses the exemptions and exceptions available under the EAR to the first two sets of controls.

8.1. Two Sets of EAR Reexport Controls Apply.

First, U.S. reexport controls apply to the reexport of products that have been exported from the United States, including parts and components incorporated into non-U.S.-made products as well as finished products. The controls apply not only to U.S. made goods, but also to non-U.S.-made products that are shipped to the United States and then reexported to another country, whether in form received or after alteration. Second, reexport controls apply to exports of non-U.S.-made products that are the direct product of specified U.S.-origin technology. This would include, for instance, a product assembled outside the United States from non-U.S. components that is based on blueprints developed in the United States. If either of these reexport controls applies, you must:

a. obtain a U.S. reexport license, or

 bflowe@bcr-dc.com

b. ensure that the U.S. controlled parts of the product are all (i) excluded from the scope of the EAR, (ii) eligible for reexport to the applicable destination with "No License Required", or (iii) eligible for reexport under a License Exception.

Thus, to be exempt from U.S. reexport licensing requirements under the EAR, the shipment must be exempt under both the rules applicable to U.S-origin items or components and those applicable to direct products of technical data and software.

8.2. Exemptions Applicable to U.S.-Origin Products.

The EAR generally prohibit reexports of commodities, software, and technology previously exported from the United States, in whole or in part, and exports of such items from the United States with the knowledge that they will be reexported from the authorized countries illegally. (See Prohibitions 1, 2, and 10, EAR Part 736.) There are several potential exceptions or exemptions to U.S. reexport licensing requirements. Their application requires a strict and careful reading of the applicable U.S. laws. The most important exemptions include:

8.2.1. No License Required. After classifying the item under the applicable ECCN set forth in EAR Part 774, determine what reasons for control are listed at the beginning of the applicable ECCN. These reasons for control correspond to columns in the Country Chart set out in EAR Part 738. Find the country of intended destination in the far-left column of the Country Chart, and move across to each of the applicable columns for the reasons for control (*e.g.*, "NS Column 1", "AT Column 1", etc.). If there is any "X" in a box, then the export requires a License or License Exception. If there is no "X" in any of the applicable boxes on the Country Chart, then no license is required for the export of that product to the applicable country as long as none of the other Prohibitions in Part 736 (not based on the product classification apply).

8.2.2. License Exceptions. Even if the Country Chart indicates a License is required, a License Exception may authorize the export. For the most part, the terms of License Exceptions set out in EAR Part 740 authorize both exports from the United States and reexports to the same end-user in the same destination in the same way. Some of these License Exception provisions apply more narrowly to reexports (*e.g.*, RPL) and some apply more broadly, so they must each be examined carefully. License Exceptions that apply based on the item characteristics as opposed to the specifics of a particular export (*e.g.,* GBS, CIV, TSU, TSR) can be most helpful in classifying a product. Pay close attention to the restrictions applicable to each License Exception before using it.

8.2.3. Reexports Covered by Specific Authorizations. A U.S. company can apply for and obtain up-front reexport authorizations on export Licenses. Also, if an existing license would cover an export from the United States, that same authorization may be used for a reexport (although it may not be used to ship more than the quantity allowed from the combined shipping points). (EAR § 740.16(c).)

8.2.4. Reexports to Country Group A:1 and Cooperating Countries. Assuming that a company's principal markets are within Country Group A:1 and cooperating

countries,[4] which includes most of the EU, the Additional Permissive Reexports (APR) License Exception allows reexporters to ship commodities for use or consumption to and among those countries without the need for a license. (EAR § 740.16(b).) This should exempt the majority of shipments by companies located in Country Group A:1 and cooperating countries from the need to obtain a U.S. reexport license, but export control staff should review this provision carefully before use.

8.2.5. Reexports to Most Other Countries Approved by Governments of Country Group A:1 and Cooperating Countries. The most useful Permissive Reexport Provision applicable to reexporters in Country Group A:1 and cooperating countries at this time is one that allows a company to make reexports to most other countries not described above based on a license or other export authorization obtained from the reexporter's government. EAR § 740.16(a) allows such exports without U.S. reexport authorization if:

> (A) the reexport is made in accordance with the conditions of an export authorization from the appropriate government export authority; and
>
> (B) the item to be reexported is *not* controlled for nuclear nonproliferation, chemical & biological weapons, missile technology, significant items (*i.e.*, hot section technology for the development, production, or overhaul of commercial aircraft engines, components, or systems), or crime control reasons; and
>
> (C) the reexport based on government authorization is either:
>
> (i) to a country in Country Group B that is not also included in Country Groups D:2, D:3, or D:4[5], and the product is controlled for national security reasons and is not controlled for export to Country Group A:1; or
>
> (ii) to a country in Country Group D:1 (except for North Korea) - and the commodities are controlled for national security reasons.

This provision has been quite controversial and subject to debate. Many think it should be expanded to provide an export license free zone for all Wassenaar Arrangement member countries as well as members of the Nuclear Nonproliferation Treaty and the Missile Technology Control Group. Hardliners think it should be eliminated entirely because it defers too much to third-country governments, but that would be a major rollback for reexport controls. It remains to be seen whether this provision lasts in its current form or is changed.

---

[4]Currently, Country Group A:1 consists of:

Australia	Belgium	Canada	Denmark	France
Germany	Greece	Italy	Japan	Luxembourg
The Netherlands	Norway	Portugal	Spain	Turkey
United Kingdom				

The "cooperating countries" are: Austria, Finland, Hong Kong, Ireland, New Zealand, South Korea, Sweden, and Switzerland. (Canada is in Country Group A, but at this point only certain nuclear specific items, chemical and biological weapon-related items, firearms, and communications intercepting items require export licenses to Canada. At some point, missile technology controlled items will also likely require a license.)

[5]Attached for your convenience are lists of these Country Groups.

 bflowe@bcr-dc.com

8.2.6. Reexports with *De Minimis* U.S. Components. Shipments of "controlled" products not covered by any of the above listed provisions, such as those to countries in Country Groups D:2, D:3, and D:4 and embargoed countries and of products controlled for nuclear nonproliferation, missile technology, and crime control reasons could still be excluded from the scope of the EAR. Certain exports of non-U.S.-made products containing *de minimis* U.S.-origin parts and components require no authorization from the United States pursuant to the so-called "parts and components" rules of EAR § 734.4. The application of those rules is quite technical, and this provision should be reviewed carefully (though some of our clients have developed computer programs to apply it). **Please note that this exclusion from the scope of the EAR does not apply to the following items: (1) shipments to a Computer Tier 3 destination of computers exceeding a Weighted TeraFLOPS ("WT") rate of 3.0 that contain U.S.-origin semiconductors (other than memory circuits) classified under ECCN 3A001; (2) shipments to Cuba, Iran, North Korea, Sudan or Syria of computers exceeding 0.002 WT containing U.S.-origin semiconductors (other than memory circuits) classified under 3A001 or high speed interconnect devices classified under ECCN 4A994.j; (3) encryption technology that incorporates U.S.-origin encryption technology classified under 5E002; (4) commercial primary or standby instrument systems classified under 7A994, commercial automatic flight control systems, or aircraft containing the same, when they integrate QRS11-00100-100/101 Micromachined Angular Rate Sensors; (5) U.S. origin technology classified at 9E003.a.1 through a.8, .h, .i, and .j (technology for certain specified gas turbine engines and components or hot section components) when redrawn, used consulted, or otherwise commingled abroad; (6) foreign made military commodities that incorporate cameras classified under 6A003.b.4.b if such cameras would be subject to the EAR as separate items and if the military commodity is not subject to the ITAR.**

(A) *De Minimis* Rules for Hardware and Combinations of Hardware and Software. The basic rules that have applied to commodities since the mid-80s are as follows. The key question for many products was what constitutes a part or component of the item that is being analyzed for *de minimis* purposes. Prior to October 1, 2008, the EAR simply gave one example, that a peripheral that is simply "rack mounted or cable connected" could not be considered a part. However, BIS had advised that telecommunications systems, for example, with components simply cable connected, could be treated as one system for *de minimis* purposes if each was an essential part and not the "principal element."

On October 1, 2008, BIS issued an interim final rule revising and clarifying the *de minimis* rule, and explained when non-U.S.-made items are not subject to the EAR. The rule, "*De Minimis* U.S. Content in Foreign Made Items," was published in (73 *Fed. Reg.* 56964 (Oct. 1, 2008).) (I initiated this rule change in 1998 on behalf of several clients and worked for 10 years in many fora to see it accomplished.) The revised rule incorporates those advisories with a clearer rule stating that a part must be "incorporated" into the non-U.S.-made item, meaning the "U.S.-origin controlled item is: Essential to the functioning of the foreign equipment; customarily included in sales of the foreign equipment; and reexported with the foreign produced item." Whether something qualifies as "incorporated" under this definition is fact-specific and often subject to interpretation, but it does not have to be inside the item. One should consider obtaining an advisory opinion from BIS in close cases.

If controlled U.S.-origin content (that which could not be exported to the applicable destination under NLR or License Exception GBS) in a European-made product is valued at 10% or less of the end-product, then no U.S. reexport authorization is needed to ship it anywhere

in the world. (OFAC regulations say less than 10% for Iran only, a fine point distinction which is only relevant if one rounds to exactly 10%.) If the U.S. content is above 10% but 25% or below, no U.S. authorization is needed unless the ultimate destination is in country group E:1 (currently Cuba, Iran, Syria, Sudan, and North Korea).

Value is determined by comparing: (i) the fair market value (usually the delivered cost) to the non-U.S. manufacturer of the controlled U.S.-origin parts, components, and materials, against (ii) the fair market value export selling price. Thus, the profit and other value added during manufacture/assembly operations essentially count as non-U.S. content. See Supplement 2 to EAR Part 734 for guidance on calculations.

Items that incorporate both software and hardware have presented difficulties for reexporters. In the past, the EAR rule was that one must do separate *de minimis* calculations, comparing hardware to hardware, software to software, and technology to technology, rather than bundling them together for purposes of these calculations. This meant that an item combining hardware, software, and/or technology had to pass each required *de minimis* test separately.

The October 1, 2008 rule modified this to allow most software "bundled" with hardware to be treated as a part or component for *de minimis* calculations. However, the rule limits what software can be treated as a bundled component to ECCNs classified as XX99X (items controlled only for antiterrorism reasons) and EAR99 items. This is a positive measure for many reexporters, but does mean software classified under ECCN 5D002 but eligible for export under License Exceptions TSU or ENC-Unrestricted to all but the AT countries cannot be treated as a bundled component.

This distinction means, for example, that Windows XP, Vista, etc., and other Mass Market products can be calculated as bundled into hardware just like other parts, but 5D002 TSU products like Linux and 5D002 ENC-U products like Windows CE, Windows XP Embedded cannot be. For products not eligible to be treated as components of hardware, the reexporter must revert to software to software, hardware to hardware, technology to technology *de minimis* calculations.

(B) *De Minimis* Rules Applicable to Software and Technology and One Time Reports. The EAR in 1996 established for the first time a clear *de minimis* exemption from U.S. reexport controls for all destinations for non-U.S. technology and software that contain less than 10% U.S. controlled content (25% for other than the U.S. Embargoed Countries). An obscure provision of the former EAR purported to control all non-U.S. technology or software if it was commingled with any level of U.S. content whatsoever. The 1996 EAR more clearly affirmed that incredibly far-reaching extraterritorial law. While that so-called "Commingling Rule" has not often been enforced and has never been tested in court (and arguably does not comply with Export Administration Act language), U.S. export enforcement officials have received much more extensive training on enforcement of technical data and software controls and have been initiating more and more cases.

In my view, the current rule made enforcement of the Commingling Rule much clearer and easier if companies did not file with BIS a mandatory report on their valuation calculations. Many practitioners had believed that Section 5(a)(5)(A) of the Export Administration Act of 1979, as amended by the Export Administration Amendments Act of 1988, already incorporated a form of *de minimis* rule applicable to software and technology (though it was not

 bflowe@bcr-dc.com

clear and was very difficult to apply). Indeed, despite language in the preamble to the 1996 EAR indicating that no such rule existed before, there existed a BIS opinion applying the old Section 5(a)(5)(A) *de minimis* rule despite the fact that BIS had not implemented it by regulation. However, the 1996 EAR rule clearly required companies to report on their valuation methodology before they may apply the *de minimis* rule in the future. If such a report was not made, then the draconian "Commingling Rule" applies regardless of the level of U.S. content. This precondition for using the new rule is due to a desire of BIS and the Defense Department to ensure that the companies' valuation accounting methods are not subject to abuse.

This rule is extremely relevant to European-made software products, a large number of which contain commingled U.S.-origin software (such as routines from run-time libraries from U.S.-origin compilers). The reporting requirement made it easier for U.S. export enforcement officers to prosecute a case under the clarified "Commingling Rule" because all that enforcement officials needed to show was (1) that a company used some U.S. content in non-U.S. software or technology exported to a country subject to unilateral U.S. controls, such as Syria, and (2) that the company failed to submit a report to BIS describing its accounting for the *de minimis* amount of such U.S. content. In that common scenario, the old "Commingling Rule" more clearly applied and the company could have been subject to the full panoply of export control penalties (including denial orders prohibiting other companies from exporting U.S. products to the company, heavy fines, and criminal penalties). To date, the number of reports under this rule that have been submitted to BIS seems to demonstrate that most ignore it.

BIS and other agencies agreed, as a policy matter, to a proposed revision to the one time report requirement for software and technology described in a proposal letter from the International Electronics Manufacturers and Consumers of America that was published in Coping with U.S. Export Controls 1996 at 767 (Practicing Law Institute ed.), which I initiated. That proposal would have allowed reexporters to defend if they could prove that their software met the *de minimis* tests after the fact, though the one time report procedure would have been maintained as a "safe harbor" preference. The BIS Office of Chief Counsel held up that change, arguing that BIS could not shift the burden of proof in an export enforcement case.

The October 1, 2008 rule resolved this problem by eliminating the requirement to file one time reports for software to qualify for *de minimis*. That is good news because otherwise, products clearly eligible for *de minimis* treatment did not qualify if no one had ever made a report. However, caution is advised because it means companies must perform their own calculations and stand behind them with no verification from the government review. The rule specifically warns of recordkeeping requirements to be able to demonstrate that the *de minimis* rule applies. Thus, we advise clients who used our model form of "one time report" to continue using it (but just for your files) to document your own *de minimis* calculations. Of course, as with all other aspects of the EAR, exporters may seek advisory opinions from BIS either formally, pursuant to EAR § 748.3(c), or informally (remembering the admonition that oral advice is worth the paper on which it is written). Few one time reports have been filed for technology, so the requirement to file one time reports for commingled technology was retained.

8.2.7. Secondary Incorporation Rule – for U.S. Parts and Components. BIS also applies a more obscure interpretation called "the secondary incorporation rule for *de minimis*" that is not well known to most exporters. This rule traditionally applied in the following limited circumstances. A U.S.-origin part or component is shipped to Country A and incorporated into Country A Built Product. That part or component is less than 25% of the

content of the Country A Built Product. The Country A Built Product is shipped to Country B (a country subject to the 25% *de minimis* rule, not the 10% rule) is not subject to the EAR because it has *de minimis* controlled U.S. content (at least with respect to Country B). In Country B, the Country A Built Product is itself incorporated into another product, Country B Built Product. There is no need to perform a *de minimis* calculation for exports of the Country B Built Product because it is not subject to the EAR (if there are no other U.S. parts or components involved). The first export remained not subject to the EAR. (However, if Country B Built Product incorporated other U.S. content ineligible for the secondary incorporation rule, a *de minimis* calculation would need to be performed for such content, but not the U.S. content incorporated in Country A.) BIS had reportedly extended this interpretation to transactions not transiting two countries, and finally published that interpretation in an Advisory Opinion on the Secondary Incorporation Rule in 2009. That Advisory Opinion also noted that, if a purchaser of parts is involved in the design of the part being incorporated and chooses the components, they would not normally be able to use the secondary incorporation rule. If they purchase the items in an arms-length transaction, they can do so.

Note that this secondary incorporation rule applies only to U.S. parts, components, and software eligible for "bundling" (not U.S. technology or un-"bundled" software) that is incorporated into a non-U.S. discrete product (not non-U.S. technology or software) as specified above. It is also different from (though somewhat similar to) the secondary incorporation rule applied to direct products of U.S.-origin technology, described below. The rationale is to minimize the burdens on non-U.S. parties who purchase such discrete products and do not normally have the ability to know how much, if any, U.S. content is incorporated.

8.2.8. Problems with Application to "Operations Software" Ameliorated. One problem with the old *de minimis* rule came when it applied to "operations software" that is not incorporated into other software but is incorporated into an end item. BIS used to advise that License Exception TSU authorized reexports of the minimum necessary operations software to run hardware items covered by the *de minimis* rules. The October 1, 2008, changes to the *de minimis* rules were initiated to correct this problem since most treat such software as another part, and now operations software classified as XD99X or EAR99 is eligible to be treated as a bundled component of the hardware. However, exporters are trying to persuade BIS to treat all software as eligible for bundling, or at least 5D002 software that is eligible for export under License Exceptions TSU and ENC-U.

8.2.9. Special Provisions Authorize Certain Exports for Servicing. A complete examination of options for servicing products exported under the *de minimis* rules is beyond the scope of this paper. Suffice it to say that reexports of U.S.-origin components in the form received must be examined to determine if a License is required. Two License Exception provisions provide some relief for reexports of controlled components. Section 740.16(h) provides License Exception APR authorization for reexports of accompanying spare parts with shipments under the *de minimis* rules:

> Shipments of foreign-made products that incorporate U.S.-origin components may be accompanied by U.S.-origin controlled spare parts, provided that they do not exceed 10 percent of the value of the foreign-made product, subject to the restrictions in Section 734.4 of the EAR.

Also, certain provisions of Section 740.10 authorize License Exception RPL to be used to export

 bflowe@bcr-dc.com

components for servicing, under strict conditions (*e.g.*, one-for-one replacements).

However, because one must also qualify reexports under OFAC rules, the application of these provisions to Country Group E is presently limited to Cuba and North Korea. For Iran and Sudan, they do not apply. The EAR does not authorize these APR provisions to be used for Syria. For those countries, exporters must find a way to export service parts at levels that qualify for *de minimis* treatment or find another alternative.

8.3. Separate Exemptions Applicable to Exports of Direct Products of U.S.-Origin Technical Data.

General Prohibition Three prohibits exports of the non-U.S.-made direct products of U.S.-origin technical data (and certain direct products of complete plants or major components of plants that are themselves direct products of U.S.-origin technical data) to destinations in Country Group D:1 (consisting mainly of the former Warsaw Pact countries) and Country Group E: destinations, unless specifically authorized by BIS by license or by regulation. (EAR § 736.2(b)(3).)[6] (Before that 2010 regulatory change, this rule did not extend jurisdiction to Iran or Sudan. 75 *Fed. Reg.* 44887 (July 30, 2010). (Query whether there is a legal defense to a company that had prior to July 2010 licensed U.S.-origin technology or software abroad, with a specific License Exception TSR written assurance, who exports direct products to Iran after the rule change. The EAR would say a license is required, but that goes beyond the scope of the company's agreement.) This rule thus does not apply to shipments to other countries.

There are also several exemptions to this rule that might apply to exports to these countries if the applicable products are made using U.S.-origin technical data. The exceptions include the following:

8.3.1. Application of Permissive Reexport Provisions. If any of the License Exceptions or other Permissive Reexport Provisions described in Part 8.2 above apply, no U.S. authorization is needed as a result of this rule either. These exemptions again should cover most shipments. (EAR § 736.2(b)(3)(iii).)

8.3.2. Product Not NS Controlled. If the product in question is not subject to

---

[6]The scope of the products and applicable technical data subject to this rule is as follows:

(A) Conditions defining direct product of technology. Foreign-made items are subject to this General Prohibition 3 if they meet both of the following conditions:

(1) They are the direct product of technology or software that requires a written assurance as a supporting document for a license or as a precondition for the use of License Exception TSR at Section 740.6 of the EAR, and

(2) They are subject to national security controls as designated on the applicable ECCN.

(B) Conditions defining direct product of a plant. Foreign-made items are also subject to this General Prohibition 3 if they are the direct product of a complete plant or any major component of a plant if both of the following conditions are met:

(1) Such plant or component is the direct product of technology that requires a written assurance as a supporting document for a license or as a precondition for the use of License Exception TSR at Section 740.6 of the EAR, and

(2) Such foreign-made direct products of the plant or component are subject to national security controls as designated on the applicable ECCN.

 bflowe@bcr-dc.com

national security controls as designated on the applicable ECCN, then no authorization is needed as a result of this rule. The foreign direct product rule does not apply to items controlled for missile technology, nuclear nonproliferation, or other reasons for control unless they are also controlled for national security reasons.

8.3.3. Non-Controlled Technology. If the technology to manufacture these products either (1) would not require a written assurance against reexport pursuant to the complex provisions for License Exception TSR (EAR § 740.6) or (2) is not subject to national security controls as designated on the applicable ECCN, no authorization is needed to export the direct product. Written assurances are required to export technology under TSR when the ECCN specifies "TSR – yes."

Whether controlled U.S.-origin technology is involved for either the plant or the products is a classification question that depends on the facts applicable to each product and plant. This question gets confusing due to one of the provisions of the General Technology Note that states: "'Technology' 'required' for the 'development', 'production,' or 'use' of a controlled product remains controlled even when applicable to a product controlled at a lower level." (EAR § 774, Supplement 2.) This statement and the remainder of the General Technology Note, combined with the mushy ECCN provisions for technology, can lead even the most expert in export controls to reach opposite conclusions.

One expert might say that since all technology to assemble controlled computers is used also to assemble computers that are not controlled, then there is no technology on our production line that is peculiarly responsible for development or production of the controlled computers. Another might say that, if a production line is capable of producing a controlled product, then it must have technology peculiarly responsible for producing the controlled product and that particular technology remains controlled even when used on the production line for producing the decontrolled products. The analysis must be taken to a deeper level than these generalities allow. The technology used by the applicable plants must be identified and classified, then, one must determine if the products of the line are the direct products of any controlled technology. Stated another way, a company needs to examine with its engineers to determine what are the specific technologies involved that are "peculiarly responsible" for producing end products that achieve technical specifications that exceed the applicable control parameters. Then, they should determine if those technologies are available in the particular plant at issue, and are used to produce the products in question. Similar analysis must be done on the technology to produce the plant, if applicable.

8.3.4. Indirect Products. Only direct products "derived immediately" from the U.S.-origin technology are subject to U.S. reexport controls, not secondary products. For instance, if a controlled set of U.S.-origin software development tools is used to create designs of motherboards, and the designs are then used to fabricate the motherboards, the designs are the direct products of U.S.-origin software but not the motherboards.[7]

[7]Unfortunately, the EAR does not currently define the term "foreign-produced direct product". However, a proposed revision of the technical data regulations published in 1988 did, and the preamble to that proposed rule stated: "The definition of 'foreign-produced direct product' of technical data and software of U.S. origin does not reflect a policy change. The examples in the proposed regulation are taken from advice BIS has given to individual exporters concerning the current definition." 53 *Fed. Reg.* 40074 (Oct. 13, 1988). That definition is "an item (commodity, technical data, or software) made in a foreign country and derived immediately from technical data or

 bflowe@bcr-dc.com

8.3.5. Incorporated Direct Products. Direct products of U.S.-origin technology that are subject to U.S. reexport controls lose their U.S. identity and are no longer subject to U.S. reexport controls when they are "incorporated" into non-U.S.-made products. This is true regardless of whether the U.S. content constitutes, say, 50% of the total value of the end-product. We should use the same definition of "incorporated" provided by example in the discussion of the parts and components rules above. Application of this exception should be made carefully. Note clearly that this "second incorporation rule" exemption only applies to the foreign-produced direct product rule, and does not apply to the *de minimis* rule.

8.3.6. Public Domain Technology. Technology on how to make products that is wholly in the public domain, including proprietary technology that is fully disclosed in patent records on file and available to the public in patent offices, which is used to make the product abroad does not subject that product to U.S. reexport controls even if the product is subject to national security controls. (See EAR § 734.7.) For example, much, if not all, technology needed to assemble Personal Computers is clearly in the public domain. The difficulty is in applying this rule to that special *je ne sais quoi* that makes a superior product.

8.3.7. *De Minimis* Technology and Software Not Subject to U.S. Reexport Control. As described above, the new EAR provides an exception for non-U.S. technology and software that contains *de minimis* U.S. content. While that provision is not directly tied to the direct product rule, if the software or technology from which the product is derived is not itself subject to the EAR, then the direct products thereof also would not be subject to the EAR.

If one can apply any or all of these rules, most and perhaps all shipments that are derived from U.S. technology may well be exempted from the U.S. EAR reexport controls on non-U.S. produced direct products. Again, one may have to be exempt under both the technical data and the product rules described above to be fully exempt.

9. Compliance with OFAC Reexport Sanctions and Embargo Controls.

This section provides further detail on the subject discussed in brief in part 5.3 above. The OFAC embargo, sanctions, and assets control regulations set forth in 31 C.F.R. Parts 500 *et seq.* prohibit most dealings with embargoed countries of any kind from the United States. Thus, to the extent that persons do business with these countries, they generally do so via non-U.S. subsidiaries or, more often, non-U.S. owned companies. This section sets forth some general compliance guidelines for the various U.S. restrictions on reexporting to, importing from, or doing business with countries or individuals subject to the embargo in the offshore transaction context. Further guidance will be required for specific transactions.

9.1. Applicable Penalties.

Penalties for violations of the rules discussed herein include, per violation, up to 10 years

---

software of U.S.-origin." The discussion above and in the next two subsections is derived from similar policy statements supported by that Proposed Rule.

 bflowe@bcr-dc.com

in prison, $1,000,000 in corporate fines, and $250,000 in individual fines[8]; denial of the privilege to ship or receive any U.S.-origin exports; and seizure and forfeiture of imported cargoes by U.S. Customs and Border Protection. Damage to a company's public image may be even more severe.

9.2. Application to More than Just "U.S. Persons".

OFAC interprets the jurisdictional coverage and reach of its regulations very broadly. In general, OFAC embargo and assets controls regulate all U.S. citizens and permanent residents wherever located, all people and organizations physically located in the United States or established under U.S. laws, and all non-U.S. branches of U.S. organizations. As discussed above, U.S. jurisdiction over non-U.S. subsidiaries of U.S. companies has long been a matter of serious international debate. OFAC regulations since the early 1980s have generally been drafted to accommodate other countries' assertions of exclusive jurisdiction over activities of non-U.S. subsidiaries of U.S. companies to engage in certain transactions as long as no U.S. person (that is, U.S. citizen, permanent resident, U.S. company or its branch office or employee or board member) is facilitating or otherwise promoting the transaction. However, the rules applicable to Cuba, still govern activities of non-U.S. subsidiaries of U.S. companies, as do new rules applicable to Iran, discussed further below.

Accordingly, most U.S. owned companies are best advised, at least initially, to treat transactions by non-U.S. branch offices and subsidiaries of U.S. companies in the same way as transactions by the U.S. offices of the company. U.S. sanctions laws applicable to some countries (such as Sudan) do contain certain exceptions applicable to non-U.S. subsidiaries. Such exceptions may allow those subsidiaries to do limited business with a proscribed country under specific circumstances. However, the application of those rules is very technical, and even the most sophisticated companies have found themselves in violation (*e.g.*, Halliburton, Caterpillar, etc.). For instance, U.S. citizens cannot be involved in transactions by a non-U.S. subsidiary, and the U.S. parent cannot exercise any control or influence on such transactions – two rules which in practice are often very difficult to follow. Also, the utility of these exceptions can be eliminated by changes in the law, as exemplified by the recent changes to the Iran Sanctions.

Even non-U.S. companies with no U.S. ownership should not consider themselves exempt from OFAC controls, despite the application of their restrictions on transactions to "U.S. Persons," since the OFAC export controls are not necessarily so limited. For example, while reexports to Iran of U.S.-origin EAR99 items that have come to rest in inventory for sale throughout the world may be permissible under the Iranian Transactions Regulations, it is illegal for a non-U.S. company to solicit a purchase from the United States with the specific intent of selling that item to Iran. Even in the case of sales from inventory, one must also comply with the EAR reexport controls in addition to the OFAC controls. The same is true for many other OFAC controls, which apply on an "in rem" basis of jurisdiction as well as "in personam".

---

[8]Under OFAC's Foreign Narcotics Kingpin Sanctions Regulations, the fines per violation can be much, much higher. Entities can be fined up to $10 million per willful violation and up to $1 million for each civil violation. Officers, directors, or agents of any entity who knowingly participate in a violation shall be imprisoned for not more than 30 years, fined not more than $5 million, or both, for each violation. These stiff sanctions were required by the Foreign Narcotics Kingpin Designation Act and suggest that it is quite likely that Congress will enact significantly larger enforcement penalties in future export control legislation than has been the case in the past.

 bflowe@bcr-dc.com

Moreover, even if a company has taken all appropriate steps to comply with such rules and prevent any unauthorized activities, engaging in lawful transactions with countries that are subject to U.S. embargoes can still create a major public image problem for the company that far exceeds the profitability of the transactions.

Accordingly, except for those cases clearly described herein, a company should only seek to use any such exceptions after careful consideration by top level officials and taking all appropriate steps to insulate any U.S. persons from such transactions.

9.3. Proscribed Countries.

Currently, U.S. law prohibits most trade transactions involving the following countries:

Cuba
Iran
North Korea
Sudan
Syria

Other countries that have been the subject of comprehensive sanctions but are no longer include Iraq and Libya.

OFAC also administers more narrowly targeted controls including, among others, those applicable to at least certain individuals of the Taliban (which formerly controlled Afghanistan), the Federal Republic of Yugoslavia (Serbia) and the Western Balkans, Burma (Myanmar), Belarus, the Democratic Republic of the Congo, Cote D'Ivoire, Iraq, the Former Liberian Regime of Charles Taylor, Zimbabwe, persons contributing to the destabilization of Lebanon, and Somalia, terrorists and their supporters, supporters of narcotics trafficking, persons involved in the proliferation of weapons of mass destruction, and property directly related to the so-called Highly Enriched Uranium Agreements between Russia and the United States. Most of these issues can be handled by screening SDNs.

Unlike the Cuba, Iran, and Sudan embargos, the provisions of the Syria embargo relating to the export and reexport of goods are not enforced by OFAC. OFAC administers the assets blocking provisions and the export of services. BIS has implemented the export control components of the sanctions by issuing General Order No. 2, as a Supplement to Part 736 of the EAR, on May 14, 2004. The General Order delineates the few items that do not require a license for Syria, what may be exported under License Exceptions, what will require a license with case-by-case consideration, and what will require a license with a policy of denial.

All License Exceptions set forth in Part 740 of the EAR are inapplicable for Syria, with the exception of portions of TMP (news media only), GOV (U.S. Government only), TSU (only for operation technology and software, sales technology, and software updates limited to bug fixes, not upgrades), BAG, and AVS (only for the reexport of civil aircraft on temporary sojourn to Syria). While TSU is available, RPL is not available for hardware replacement parts, so many companies are applying for licenses for servicing hardware.

All other exports and reexports of items subject to the EAR are subject to a general policy of denial, with the exception of certain items BIS may consider on a case-by-case basis, including

 bflowe@bcr-dc.com

(1) items necessary to conduct U.S. foreign and military affairs, and in support of activities, diplomatic or otherwise, of the U.S. Government; (2) medicine (on the CCL) and medical devices (both as defined in Part 772 of the EAR); (3) parts and components intended to ensure the safety of civil aviation and the safe operation of commercial passenger aircraft; and aircraft chartered by the Syrian Government for the transport of Syrian Government officials on official Syrian Government business; (4) telecommunications equipment and associated computers, software and technology; and (5) items in support of United Nations operations in Syria.

Of course, OFAC has jurisdiction over the freezing of Syrian assets. On August 1, 2007, President Bush issued an Executive Order blocking the property and property interests of individuals, entities, and other persons who undermine the sovereignty of Lebanon or its democratic processes or institutions. (72 *Fed. Reg.* 43499 (Aug. 3, 2007).)

More recently, on August 11, 2011, and in the wake of violent repression by the Assad regime, President Obama issued Executive Order 13582 blocking (freezing) all Syrian Government assets under U.S. jurisdiction and barring U.S. persons from providing any services to or investments in Syria, and facilitation of the same. The Executive Order also prohibited importation into the United States of petroleum or petroleum products of Syrian origin, and any transaction or dealing by a U.S. person in or related to such products. Updates on recent developments in the sanctions against Syria are covered in Section 13.

The Sudan sanctions target the Government of Sudan, blocking its property, and prohibiting U.S. persons from engaging in or facilitating trade-related transactions involving Sudan. Controls on U.S.-origin goods are also subject to conjointly administered (BIS and OFAC) export and reexport controls under the EAR.

While OFAC long ago amended its rules to exclude the areas now comprising the new nation of South Sudan from OFAC sanctions, many transactions with South Sudan involved ancillary activities via Sudan (i.e., northern Sudan) that still required an OFAC license, such as any oil and gas related transactions, transportation through Sudan to South Sudan (which has no ports or major airports), and many banking activities.

On December 8, 2011, OFAC revised its Sudanese Sanctions Regulations ("SSR") (31 C.F.R. Part 538) to eliminate most OFAC licensing requirements on such ancillary activities. 76 *Fed. Reg.* 76617 (Dec. 8, 2011). In its final rule, OFAC made two main changes: (1) added a new SSR § 538.536 to authorize virtually all activities and transactions relating to the petroleum and petroleum industries in South Sudan, and (2) added a new SSR § 538.537 to authorize the transit or transshipment of goods, technology, and services through Sudan to or from South Sudan. Among other things, new SSR § 538.536 authorizes the transshipment of goods, technology, and services relating to petroleum industries to or from South Sudan through Sudan, but does not authorize the refining in Sudan of petroleum from South Sudan. Financial transactions ordinarily incident to the activities authorized by SSR §§ 538.536 and Part 537 are also authorized, subject to certain limitations.

While the revised SSR greatly simplifies compliance concerning transactions with South Sudan, it still would be easy to violate the SSR inadvertently while doing business with South Sudan. Care therefore must be taken to ensure that OFAC and BIS licenses are not needed or that you obtain licenses that are required.

 bflowe@bcr-dc.com

Exports/reexports to South Sudan that are subject to U.S. jurisdiction continue to be required to comply with other applicable U.S. export controls, such as the EAR and the ITAR. Also, Sudan (northern Sudan) continues to be subject to a U.S. embargo, which is administered mainly by OFAC, BIS, and DDTC.

Like the Syria embargo, the export and reexport provisions of the U.S. embargo on North Korea are enforced by BIS, not OFAC. The North Korea Sanctions prohibit all unlicensed exports of items subject to the EAR (including EAR99 items except for EAR99 food and medicine). Furthermore, the sanctions target a number of key North Korean entities on the OFAC SDN list under non-proliferation based sanctions programs and subject to target EAR license requirements. Aside from BIS restrictions on exports and reexports, OFAC sanctions prohibit imports from North Korea.

The Cuba and Iran sanctions are the most comprehensive and prohibitive of the OFAC sanctions regimes. They essentially prohibit all trade with Cuba and Iran and are discusses in further detail in Section 9.8 below.

9.4. Restrictions On Nationals and "Specially Designated Nationals".

9.4.1. Nationals of Sanctioned Countries. Most of the OFAC restrictions apply not only to dealings with the countries themselves, but also to transactions with nationals of such countries (including corporations and other forms of business organized under their laws) and with certain "Specially Designated Nationals" ("SDNs") who may be located in third countries, such as several prominent Iranian banks. It is just as illegal to transact business with those SDN entities as to do so directly with the restricted countries. In fact, if such an entity is involved in a transaction, a company could face problems regardless of whether the company transacts business with it directly.

9.4.2. Narcotics Traffickers and Terrorists. OFAC's SDN lists also include designated narcotics traffickers and terrorists. Each are directed against individuals and entities involved in such activities anywhere in the world. As a practical matter, for many companies the designated narcotic traffickers are the most significant parties on the various denial lists because they include substantial companies with tremendous resources, not merely smaller companies who have defaulted in an export enforcement case.

Confusingly, the sanctions against narcotics traffickers are implemented in two different OFAC programs, the Narcotics Trafficking Sanctions Regulations ("Trafficking Regulations") and the Foreign Narcotics Kingpin Sanctions Regulations ("Kingpin Regulations"). The Trafficking Regulations, 31 C.F.R. Part 536, implement sanctions against individuals and entities connected to narcotics trafficking centered in Colombia. The Kingpin Regulations, 31 C.F.R. Part 598, are directed against narcotics trafficking worldwide, not just those activities connected to Colombia. Sanctioned parties under both the Kingpin and Trafficking Regulations are known as Specially Designated Narcotics Traffickers; however, such persons are differentiated on OFAC's consolidated list of SDNs with "SDNTK" signifying those listed pursuant to the Kingpin Regulations and "SDNT" for those designated under the Trafficking Regulations. Persons listed as SDNTs pursuant to the Trafficking Regulations are not affected by the Kingpin Regulations.

The sanctions against SDNTKs are virtually identical to those against the

 bflowe@bcr-dc.com

SDNTs, Specially Designated Terrorists, Specially Designated Global Terrorists (and other SDNs). The Kingpin Regulations block all property and interests in property of SDNTKs in the United States or within the possession or control of any U.S. person. The regulations prohibit transactions or dealings by U.S. persons, or within the United States, in property or interests in property of SDNTKs and also prohibit transactions or dealings by U.S. persons, or within the United States, to evade or avoid the regulatory prohibitions. However, civil and criminal penalties for violations of the Kingpin Regulations are significantly larger than those for violations of any other OFAC sanctions program, including the Trafficking Regulations. For example, entities can be fined up to $10 million per willful violation of the Kingpin Regulations and up to $1 million for each civil violation. Officers, directors, or agents of any entity knowingly participating in a violation shall be imprisoned for not more than 30 years, fined not more than $5 million, or both, for each violation. Other penalties are set forth in 31 C.F.R. § 598.701. These stiff sanctions were required by the U.S. legislation and suggest that it is quite likely that Congress will enact significantly larger enforcement penalties in future export control legislation than has been the case in the past.

By Executive Order 13224 on September 23, 2001, President Bush imposed additional sanctions on terrorists and their supporters. Under the Executive Order, President Bush blocked all assets of designated foreign terrorists and those who assist them. The blocking extends to property interests of designated terrorists that are in the United States, that enter the United States, or that come within the possession or control of U.S. persons. The term "U.S. person" is defined as "any United States citizen, permanent resident alien, entity organized under the laws of the United States (including foreign branches [but not foreign subsidiaries]), or any person in the United States".

The Annex to the Executive Order listed several individuals and entities subject to the blocking order, including the late Osama bin Laden and his chief lieutenants. Since then, numerous additional individuals and entities have been added to this denial list. Exporters have added the parties sanctioned under the Executive Order to the lists of denied persons. Also subject to the blocking order are:

- Foreign persons determined by the Secretary of State to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States;

- Persons determined by the Secretary of Treasury to be owned or controlled by, or to act for or on behalf of any persons listed under the Order or any other persons determined to be subject to it;

- Persons determined by the Secretary of Treasury to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed under the Order or determined to be subject to it;

- Persons determined by the Secretary of Treasury to be otherwise associated with those persons listed under the Order or determined to be subject to it.

The Executive Order's other key prohibitions include:

- No transaction or dealing by U.S. persons (including their overseas branches, but not their foreign subsidiaries) or within the United States in blocked property.

- Prohibition against U.S. persons or persons in the United States from evading or avoiding, or attempting to evade or avoid any of the Order's prohibitions.

- Prohibition against any conspiracy to violate any of the Order's prohibitions.

- Prohibition against donations intended to relieve human suffering to persons listed under the Order or determined to be subject to it.

As a practical matter, these terrorist sanctions largely overlap previously existing U.S. terrorist sanctions administered by OFAC, *i.e.*, the Terrorism Sanctions Regulations (31 C.F.R. Part 595) and the Foreign Terrorist Organizations Regulations (31 C.F.R. Part 597). Under the Terrorism Sanctions Regulations, OFAC has blocked the property of persons posing a significant risk of disrupting the Middle East peace process. Under the Foreign Terrorist Organizations Regulations, OFAC requires U.S. financial institutions to block all funds in which foreign terrorist organizations have an interest.

Most of the persons listed in the Annex to President Bush's September 23, 2001 Executive Order were already listed as Specially Designated Terrorists under Part 595 or as Foreign Terrorist Organizations under Part 597. However, the sanctions extended pre-existing sanctions in important ways. First, they are broader than the Terrorism Sanctions Regulations in that they are not limited to terrorists that pose a significant risk of disrupting the Middle East peace process. Second, they are broader than the Foreign Terrorism Organization Regulations in that they require blocking actions by all U.S. persons, not just U.S. financial institutions. Third, the sanctions make it easier to designate terrorists because anyone "associated" with terrorists can be listed. OFAC has used this provision to block the U.S. assets of, and bar U.S. market access to, foreign banks that are linked to terrorists and which have refused to freeze terrorists' assets.

In the past, the United States has had difficulty in convincing its allies and foreign banks to impose sanctions on terrorists. The terrorist attacks of September 11, 2001, however, resulted in far greater international cooperation in this area. The imposition of comprehensive sanctions on terrorists by the United Nations Security Council have also contributed to increased cooperation. (Resolution 1373, September 28, 2001.)

For legal reasons (and also obvious moral ones), foreign subsidiaries of U.S. companies should not deal with terrorists. While they appear to be beyond the scope of the Executive Order, any link between a foreign subsidiary and a terrorist could be treated as an "association" warranting sanctions.

9.5. Prohibited Activities.

The following types of activities are generally prohibited by OFAC regulations:

9.5.1. Imports. Goods or services originating from proscribed countries may not be imported into the United States either directly or through third countries unless licensed by OFAC.

 bflowe@bcr-dc.com

9.5.2. Contracts in Which Proscribed Countries or Their Nationals Have an "Interest" (broadly interpreted) are prohibited unless licensed by OFAC. Such contracts can include remote interests, such as on a brokerage contract, or a service contract with an oil company related to its work in the offshore waters of a proscribed country.

9.5.3. Exports. Except for "informational materials", no products, technology, or services may be exported to proscribed countries, either directly or through third countries, unless licensed by BIS or OFAC by specific license or by regulation. (However, OFAC recently issued a General License authorizing the export of food to Iran and Sudan, as discussed in Section 13.3.1.7.)

Many requests for licenses are subject to a general policy of denial. However, the Trade Sanctions Reform and Export Enhancement Act of 2000 ("Trade Sanctions Reform Act" or "TSRA") essentially established a favorable licensing policy for exports and reexports of agricultural commodities, medicines, and medical products to countries designated as supporters of international terrorism by the Secretary of State. Presently, the designated countries are Cuba, Iran, Sudan, and Syria.

9.5.4. Payments. For licensed transactions, documents must reference a specific license issued by OFAC or a license issued by Commerce.

9.5.5. Travel. For some countries such as Cuba, special permission is required to travel there. In the case of other countries, there is no need for special permission for travel, but there are often tight restrictions on permissible activities while in the country.

9.5.6. Bank Accounts and Other Assets. Any dealings in assets or financial dealings with proscribed countries or their nationals generally require specific licenses (except for generally authorized travel-related transactions and trade in informational materials).

9.6. Letters of Intent and Discussions Permitted but Not Binding Contracts.

Informational exchanges, business discussions, and non-binding letters of intent are generally permissible in all countries. However, binding contracts, even conditioned upon obtaining all required U.S. licenses, are generally prohibited as to "U.S. persons" without a specific license or regulatory exception.

9.7. Licensing under OFAC Regulations.

OFAC has a similar licensing structure to that in place at BIS. The general license is a regulatory provision that authorizes a certain range of transactions. One does not always see the words "general license" in the regulations. Instead, OFAC often signals a general license by use of the words "is authorized", "exempt from the prohibitions and regulations" or "excepted from the prohibitions of this part". Usually general licenses are contained in Subpart E for each set of regulations.

In contrast, the regulations usually expressly state when a specific license must be requested. OFAC will issue a specific license (the counterpart to BIS's License) on a case-by-case basis. Applications for specific licenses must take the form of an application, signed by the applicant, which explains why the license should be granted. See 31 C.F.R. Part 501 for license

application and reporting procedures. Specifically the letter must:

- Supply all requested information;
- Disclose the names of all concerned or interested parties and if filed by an agent, disclose the names of all principals;
- Attach all relevant documents.

Unless the application is for a license to export agricultural commodities, medicines or medical products, which may now be submitted online, the application letter must be mailed or physically delivered to OFAC as the office will not process faxed applications.

9.8. Controversial U.S. Unilateral Sanctions.

This subsection discusses the Cuban Liberty and Democratic Solidarity Act of 1996 (popularly known as the "Helms-Burton Act") (22 U.S.C. § 6021 *et seq.*) and the Iran and Libya Sanctions Act of 1996 ("ILSA")) (50 U.S.C. § 1701 note), which have probably caused more friction between the United States and its European allies than any other U.S. unilateral sanctions measures. In response to vociferous criticism from and countermeasures by U.S. allies, President Clinton greatly reduced the impact of both laws by exercising waiver or suspension rights, as have subsequent Presidents. Not surprisingly, this outraged many of the sanction laws' supporters in Congress.

9.8.1. Helms-Burton Act. Helms-Burton legislation initially appeared unlikely to be enacted until it proved a convenient response to Cuba's shooting down of two civilian airplanes. The legislation was then quickly passed to strengthen U.S. sanctions on Cuba. The fact that the U.S. sanctions on Cuba already amounted to a near total embargo explains why it was difficult to pass stronger legislation without damaging relations with U.S. allies. Helms-Burton extended the extraterritorial reach of U.S. sanctions in two ways. First, under Title III, it created a private right of action for U.S. nationals to recover damages in U.S. courts from non-U.S. persons who are "trafficking" in property belonging to the plaintiff that was confiscated by the Cuban Government on or after January 1, 1959. Damages can equal the amount certified by the Foreign Claims Settlement Commission plus interest, the amount determined by a special master appointed by a court, or the fair market value of the confiscated property. Second, under Title IV, the Act requires the U.S. Government to deny entrance into the United States by non-U.S. nationals who "traffic" in confiscated property that is the subject of a claim by a U.S. person. The exclusion must also apply to any spouses, minor children, or agents of non-U.S. nationals involved in "trafficking". "Trafficking" is defined broadly and includes dealing in confiscated property or engaging in a commercial activity using or otherwise benefitting from such property (but not passive stock ownership in a company said to be trafficking).

Under authority provided by the Act, the Clinton Administration continually suspended the right of U.S. nationals to bring suit under Title III, as have the Bush and Obama Administrations. A new waiver or suspension is required every six months.

9.8.2. Iran Libya Sanctions Act and Comprehensive Iran Sanctions, Accountability, and Divestment Act.

9.8.2.1. Iran Libya Sanctions Act ("ILSA"). ILSA mandated sanctions against non-U.S. companies and sometimes their affiliates for making certain petroleum-related investments in Iran (and originally in Libya). More specifically, the statute required the President to impose at least two of seven listed sanctions against non-U.S. persons who knowingly make an investment of $40 million or more that directly and significantly contributes to the enhancement of Iran's ability to develop its petroleum resources. Investments in Libya are no longer subject to sanctions.

The ILSA menu of sanctions available to the President included: (1) denial of licenses for exports and reexports to the sanctioned party, (2) denial of Export-Import Bank assistance for exports to the sanctioned party, (3) ban on U.S. government procurement of goods or services from the sanctioned party, (4) prohibition on imports from the sanctioned party, (5) ban on U.S. financial institutions making loans or providing credits in excess of $10 million (in any one-year period) to the sanctioned parties, (6) (for a sanctioned party that is a financial institution) prohibition on service by the sanctioned party as a primary dealer in U.S. government bonds, and (7) (for a sanctioned party that is a financial institution) preclusion of service by the sanctioned party as a repository of U.S. government bonds.

On August 3, 2001, ILSA was extended for five years with minor modifications. In the wake of the referral of Iran to the U.N. Security Council for their nuclear activities, on September 30, 2006, President Bush signed into law the Iran Freedom Support Act ("IFSA"), which revised and extended ILSA for five more years, through December 31, 2011. Presidents never imposed sanctions under either Act, but many companies withdrew investments in the face of potential sanctions.

9.8.2.2. Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"). Before IFSA expired, sanctions were extended and toughened greatly by CISADA. CISADA focused new sanctions on the purchase of refined petroleum by Iran and of goods, services, and materials used to modernize Iran's oil and natural gas sector. CISADA is also intended to make it more difficult for the Iranian Revolutionary Guard Corps ("IRGC") and Iranian banks to support Iran's nuclear program and terrorism and to engage in international finance. CISADA imposes new certification requirements on companies seeking new contracts with the United States. Also, CISADA prohibits funding and development of Iran's nuclear program and imposes sanctions on individuals who commit serious human rights violations. There is a specific exemption under CISADA for technology and services which allow Iranian individuals access to information and to communicate freely, primarily through social network services.

9.8.2.2.1. Sanctions Apply to "Investments" in Iran's Petroleum Related Resources. CISADA continued existing extraterritorial sanctions involving $20 million or more of "investments" that directly and significantly contribute to the enhancement of Iran's ability to develop petroleum resources, and expanded such sanctions to apply to imported refined petroleum to Iran, and other refined petroleum products in Iran. CISADA imposed punitive sanctions against any party (U.S. and non-U.S.) that supplies, or supports the supply of, refined petroleum products to Iran or facilitates development of Iran's domestic refining capacity. CISADA clarified and expanded the scope of parties that may be subject to punitive action for violations, including non-U.S. Persons whose activities otherwise were not subject to U.S. extraterritorial jurisdiction. CISADA required the President to impose sanctions against any person who knowingly does any of the following:

 bflowe@bcr-dc.com

a. Makes an "investment" of $20 million or more (or any combination of investments where the total adds up to this amount in a 12-month period) that directly or significantly contributes to Iran's ability to develop its own petroleum resources. The term "petroleum resources" includes petroleum, refined petroleum products, oil or liquefied natural gas, natural gas resources, oil or liquefied natural gas tankers, and products used to construct or maintain pipelines used to transport oil or liquefied natural gas; or

b. Provides goods, services, technology, information, or support that could directly and significantly facilitate Iran's maintenance or development of its domestic refined petroleum production capacity. This prohibition covers a single event worth $1 million or more (or any combination of activities that total at least $5 million over a 12-month period). Refined petroleum products include diesel, gasoline, jet fuel, and aviation gasoline. This restriction could be triggered by just the maintenance of existing facilities which meet the criteria; or

c. Sells or provides refined petroleum products to Iran, or any goods, services, technology, information, or support that could directly and significantly contribute to the enhancement of Iran's ability to import refined petroleum products. This restriction applies to any activity worth $1 million or more (or multiple activities worth at least $5 million together over a 12-month period). There are limited exceptions to this restriction for certain underwriting, insurance, or reinsurance activities, however the exception applies only if the President determines that the person has exercised due diligence in establishing and enforcing official policies, procedures, and controls to ensure that the person does not underwrite or enter into a contract to provide insurance or reinsurance for the sale, lease, or provision of goods, services, technology, information, or support to Iran.

These restrictions will apply directly to more non-U.S. companies on an extraterritorial basis as the definition of "persons" covers financial institutions, insurers, underwriters, guarantors, or any other business organizations, including a parent and its foreign subsidiary or affiliate. CISADA includes in its reach (a) successors in interest to an entity that engaged in a prohibited activity; (b) persons that own or control the entity that engaged in such activity, if they knew or had reason to know the violation occurred; and (c) entities owned or controlled by, or under common ownership with, the sanctionable entity that knowingly engaged in sanctionable conduct. This was an extension of pre-existing laws, as it provided for potential imposition of sanctions on companies affiliated with a sanctionable entity even if they are not subject to the ownership or control of that entity.

CISADA changed the definition of "investment" under ILSA to include within the definition the performance or financing of a contract to sell or purchase goods, services, or technology and not just equity, debt, or royalty participation in the development or the petroleum resources of Iran, which was the previous standard. The Act made this change indirectly by deleting the prior law's exception for "the entry into, performance, or financing of a contract to sell or purchase goods, services, or technology." (Oddly, Section 202 (g)(2)(C) of CISADA authorizing state and local divestment, described below, more specifically includes within its definition of "investment" the "entry into or renewal of a contract for goods or services." The legislative history of Section 102 of CISADA makes clear that the deletion of the exemption is intended to accomplish the same result.) CISADA also confirmed this revised

 bflowe@bcr-dc.com

definition of "investment" by striking references in ISA from "investment activity in Iran" to merely "activity" in Iran. Fortunately, CISADA somewhat narrowed the application to contracts of sale because they, like all investments, must "directly and significantly contributes to the enhancement of Iran's ability to develop petroleum resources" or "that could directly and significantly facilitate the maintenance or expansion of Iran's domestic production of refined petroleum products, including any direct and significant assistance with respect to the construction, modernization, or repair of petroleum refineries.

Thus, the long-standing reexport exemptions for U.S.-origin products that are EAR99 in non-U.S. inventory or less than 10% U.S.-origin content, as long as no U.S. person is involved (complex areas on which we can advise further), still apply; nevertheless, these new sanctions can apply even to those otherwise not prohibited reexports and others where there are no U.S. contacts.

9.8.2.2.2. Menu of Sanctions. CISADA added the following three additional sanctions to the six that the President already has at his disposal to choose from to sanction violations of CISADA. The new penalties available are:

a. Prohibit any transactions in foreign exchange that are subject to the jurisdiction of the United States and in which the sanctioned person has any interest;

b. Prohibit any transfers of credit or payments between financial institutions or by, through, or to any financial institution, to the extent that such transfers or payment are subject to the jurisdiction of the United States and involve any interest of the sanctioned person; and

c. Prohibit any person from acquiring, holding, withholding, using, transferring, withdrawing, transporting, importing, or exporting any property that is subject to the jurisdiction of the United States and with respect to which the sanctioned person has any interest or dealing in or exercising any right, power, or privilege with respect to such property, or conducting any transaction involving such property (seems likely to be implemented by blocking orders, making persons effectively SDNs).

9.8.2.2.3. Mandatory Investigations and Presidential Waiver Authority. CISADA restricted the President's right to waive the application of the sanctions and imposed a requirement on the President to report to Congress on his efforts to prevent foreign persons from engaging in sanctionable activities. The President must establish that a waiver is "necessary to the national interest" instead of the prior standard of "important to the national interest." Such waivers are only good for twelve months, but can be renewed for subsequent six-month periods. CISADA also provided the President with authority to issue limited waivers based upon his certifying that the country of primary jurisdiction over the party is closely cooperating in multilateral efforts to prevent Iran from acquiring or developing chemical, biological, or nuclear weapons and that it is "vital to the national security interests." The President must also submit a report to the appropriate Congressional committees justifying the waiver.

Instead of allowing the President discretion to institute investigations of violations of ILSA, CISADA imposed an obligation on the President to investigate potential

violations of CISADA "for which there is credible evidence." (Presumably, a determination by the State Department as to whether credible evidence exists, a standard not very high but not very clear, either, is required for them to initiate an investigation and start the "clock.") There is a special provision that the President need not initiate an investigation and may terminate an investigation if the President certifies in writing to the appropriate congressional committees that (i) the person whose activity was the basis for the investigation is no longer engaging in the activity or has taken significant verifiable steps toward stopping the activity and (ii) the President has received reliable assurance that the person will not knowing engage in an activity in the future.

9.8.2.2.4. Financial Institutions. CISADA imposed broad new restrictions on "foreign financial institutions" and "domestic financial institutions." CISADA clearly expressed the intent to attempt to drastically restrict access of the Government of Iran, Iranian banks, Iranian SDNs, and the IRGC to international financial services in a continuing effort to punish these entities for their proliferation related activities or their support of terrorist organizations.

The major impact on U.S. financial institutions is CISADA's requirement for them to conduct "audits" on certain non-U.S. financial institutions with which they do business and provide "certifications" relating to their interaction with foreign financial institutions. CISADA was clearly attempting to expand the extraterritorial reach of the United States by imposing obligations on U.S. regulated financial institutions that can only be met by extending those obligations to those foreign banks that have or want a correspondent relationship with U.S. banks. The three basic elements of the financial regulations are:

a. Imposition of conditions on correspondent or payable-through accounts in the U.S. of foreign financial institutions that i) facilitate the Iranian Government's efforts to acquire weapons of mass destruction or support international terrorism; ii) deal with Iranian companies sanctioned by the United Nations; iii) engage in money laundering activities associated with efforts to acquire weapons of mass destruction or support international terrorism; iv) facilitate the Central Bank of Iran in any restricted activities; and v) facilitate any activities by the IRGC.

b. Prohibition on transactions with the IRGC by foreign-owned or controlled affiliates of U.S. financial institutions and subject those entities to potential penalties. In addition U.S. parent institutions are now made expressly subject to penalties under the Iranian Transactions Regulations if they have knowledge or reason to know that any entity that they own or control engages in such transactions.

c. Imposition of new requirements on U.S. financial institutions which maintain correspondent or payable-through accounts with foreign financial institutions. The U.S. financial institution must:

   i. Perform audits of such accounts for violations of the Act;
   ii. Report to OFAC transactions or financial services involving any specially designated Iranian banks;
   iii. Certify, to the best of its knowledge, that the foreign financial institution is not knowingly engaging in any prohibited activity; and

 bflowe@bcr-dc.com

iv. Establish due diligence policies, procedures and controls, reasonably designed to detect whether the foreign financial institution knowingly engaged in prohibited activity.

These provisions were clearly designed to force non-U.S. financial institutions to choose between doing business with U.S. banks or Iranian banks. U.S. banks are now required to investigate their non-U.S. correspondents as the U.S. banks have an affirmative obligation to determine whether a non-U.S. financial institution is doing anything which may violate CISADA. The U.S. banks will have an obligation to ask non-U.S. financial institutions with which they have correspondent relationships for their certification that the non-U.S. financial institution in not involved in any transaction with a designated Iranian bank. Most major non-U.S. financial institutions have apparently been involved with oil sales and purchases that require them to deal with designated Iranian banks. If the non-U.S. financial institution is not able to provide the certification required by CISADA, the U.S. financial institution will have to decide whether to terminate its correspondent relationship. Thus, the U.S. Government is using U.S. banks to monitor, and eventually reduce, Iranian banks' access to the international banking system.

Many non-U.S. banks have decided to cease doing business with Iran in the last few years after ABN Amro, UBS, Credit Suisse, Lloyds, Barclays and others were hit with tens to hundreds of millions in fines to various U.S. Government agencies for allegedly pushing Iranian transactions through the U.S. banking system after "stripping" out all references to Iran. Other major international banks may follow this trend.

The Iranian Financial Sanctions Regulations ("IFSR") implement Section 104(c) of CISADA, which imposes strict conditions on the opening and maintaining in the U.S. of a correspondent account or a payable-through account by a non-U.S. financial institution which is found to knowingly engage in activity which facilitates certain activities of the Government of Iran or the IRGC. The IFSR also implements Section 104(d) of CISADA, which prohibits any person owned or controlled by a domestic financial institution from knowingly engaging in a transaction with or benefitting the IRGC. The thrust of the obligation is for OFAC to list such institutions as SDNs in Appendix A to new 31 C.F.R. Part 561 (which is now empty and reserved), and then prohibit any person owned or controlled by a U.S. financial institution from knowingly engaging in transactions or benefitting the IRGC or other blocked persons based on such OFAC finding and SDN listing. (IRGC parties are already listed under other sanctions.) The IFSR also allows the Secretary of the Treasury to issue absolute prohibitions precluding a U.S. financial institution from opening or maintaining U.S. correspondent accounts or payable-through accounts for a non-U.S. institution that is found to knowingly engages in any of the following activities: i) facilitates the Government of Iran or the IRGC to acquire or develop weapons of mass destruction or support acts of international terrorism; ii) facilitates activities of person subject to U.N. financial sanctions; iii) engages in money laundering; iv) facilitates prohibited activities of the Central Bank of Iran or other Iranian banks; and v) facilitates significant transactions of the IRGC or that of blocked entities

9.8.2.2.5. Nuclear, Chemical, or Biological Weapons Sanctions on Exports to Countries with Jurisdiction over Proliferation. CISADA provided that no U.S. license or other approval may be issued for export, transfer, or retransfer of nuclear materials, components, facilities or other goods, services , or technology subject to a U.S. nuclear cooperation agreement to a country with primary jurisdiction over a person subject to sanctions

 bflowe@bcr-dc.com

for activities on or after enactment of CISADA that contributes to Iran's nuclear, chemical, or biological weapons capabilities or that contributes to disruptive levels of conventional weapons procurement by Iran. There is limited waiver authority given to the President which he can exercise if he notifies Congress that a) the government of the country affected did not know or have reason to know of the activity; and b) the country is taking all reasonable steps both to prevent a recurrence and to penalize the sanctioned person. In addition, the President can waive the restrictions on a case-by-case basis by making a determination that such action is vital to the national interest and issuing a report to Congress providing justification for the decision.

9.8.2.2.6. Other Significant Provisions. CISADA includes a number of other prohibitions or restrictions that merit mention here. For example, CISADA also:

- Removes authorization for imports of Iranian carpets, caviar, pistachio nuts, etc., to the United States.
- Prohibits U.S. government agencies from entering or renewing a contract with a person that exports "sensitive technology" to Iran, defined as any hardware, software, telecommunications equipment or any other technology that the President determines is to be used specifically to restrict the free flow of unbiased information in Iran or to disrupt, monitor, or otherwise restrict speech of the people of Iran.
- Requires a certification from every prospective U.S. government contractor that they and any person owned or controlled by the person, does not engage in any activity for which sanctions may be imposed.
- Authorizes state and local governments to divest from, or prohibit investment of their assets in, any company that it determines engages in certain investment activities in the energy sector of Iran.
- Requires the Director of National Intelligence to prepare a list of countries that allow the diversion of U.S.-origin goods, services, or technology to Iranian end-users or intermediaries. The President is then required to designate a country a "Destination of Diversion Concern" if the country is considered to allow a substantial diversion of goods, services or technology to Iran, based upon: a) the volume of goods, services, and technology diverted to Iran; b) the inadequacy of the country's export controls; c) the country's unwillingness or inability to control the diversion; and d) the country's unwillingness or inability to cooperate with the United States in efforts to stop the diversion.

More recent developments in Iran sanctions are explained in detail in Section 13.3 below.

9.8.3. <u>Responses of European Union and Other U.S. Allies</u>. Enactment of Helms-Burton and ILSA created a firestorm of controversy with U.S. allies, particularly the EU and its member states, Canada, and Mexico, who claimed that the laws infringed on their sovereignty and violated international law. The EU passed a regulation to block compliance with the Acts (and also with certain other U.S. sanctions against Cuba) in its territory and to allow its citizens and companies to recover any damages caused by application of the sanctions. (Council Regulation (EC) No. 2271/96, 36 I.L.M. 125 (1997).) Canada and Mexico enacted comparable laws to counteract Helms-Burton. These U.S. sanctions and non-U.S. blocking statutes create situations where individuals and companies can violate U.S. law by complying with the applicable non-U.S. law and vice versa. In such situations, both U.S. and non-U.S. companies should exercise great care and work with counsel skilled under both laws to avoid potential liability in the United States and other country(ies) involved.

 bflowe@bcr-dc.com

In October 1996, the EU initiated World Trade Organization ("WTO") dispute settlement proceedings challenging the legality of the Helms-Burton Act and the U.S. embargo of Cuba. Canada participated as a third-party in the case. The United States took the position that the dispute involved national security and foreign policy issues beyond the scope of the WTO. Based on the possibility of successful negotiations with the United States, the EU suspended the case in April 1997. In April 1998, the case expired, although the EU has the right to initiate another one. In May 1998, the United States and the EU reached an agreement to resolve the dispute. The EU agreed not to revive its WTO case so long as the United States did not impose any penalties on EU companies under either Act. The agreement exempted Total, a French oil company, from any sanctions for its participation in a $2 billion oil and gas investment project in Iran. (Sanctions also were not imposed on Total's partners in the deal, Gazprom of Russia and Petronas of Malaysia.) The United States also committed to amend the Helms-Burton Act to provide waiver authority to Title III's exclusion provisions and to modify the ILSA to provide expanded waiver authority. The agreement provided for the creation of a global registry of expropriated properties in dispute. Companies that invest in legitimately disputed properties would be denied financial assistance, export credits, and any other government assistance. According to Leon Brittan, then the EU Trade Commissioner, the registry would not cover investments that had already been made by European companies in Cuba.

Since the 1998 agreement with the EU, the United States has neither amended the Helms-Burton Act to provide waiver authority to Title III's exclusion provisions nor amended the ILSA to provide expanded waiver authority. Indeed, CISADA restricts the President's right to waive the application of the sanctions and imposes a requirement on the President to report to Congress on his efforts to prevent foreign persons from engaging in sanctionable activities.

9.9. Permitted Offshore Activities Involving Iran and Sudan.

OFAC controls generally prohibit all meaningful business involving Iran or Sudan by U.S. companies. The complexities of the Iranian Transactions and Sanctions Regulations ("ITSR") (31 C.F.R. Part 560) involve what types of activities by non-U.S. persons are permissible.

All restrictions apply to "U.S. persons", which include U.S. citizens and permanent residents wherever located and U.S. branch offices in other countries. Recent changes to the sanctions also extend the Iran sanctions to non-U.S. subsidiaries of U.S. companies. Additionally, prohibitions apply to reexports of U.S.-origin items regardless of whether made by U.S. persons. They include reexports to the "Government of Iran."

A noteworthy trap for unwary U.S. persons is set forth in Section 560.208 of the ITSR, which prohibits U.S. persons, wherever located, from "facilitating" transactions of the non-U.S. persons where such transactions would be prohibited if performed by a U.S. person. The ITSR do not provide a definition of facilitating or its variants. However, the facilitation provisions prohibit as examples U.S. persons from approving, financing, or guaranteeing permitted activities by non-U.S. persons if it would be illegal for the U.S. person to engage in any such activity itself. Further, as described in Section 560.417, facilitation includes a U.S. person altering its operating policies or procedures, or those of a foreign affiliate, to permit acceptance or performance of a specific contract, engagement or transaction involving Iran or Government of Iran without the approval of the U.S. person, if approval would have previously been required and if the activity would be prohibited for U.S. persons. Section 560.417 also describes the facilitation prohibition

 bflowe@bcr-dc.com

as including the referral to foreign persons of purchase orders, requests for bids, or similar business opportunities to which the U.S. person could not directly respond, or changing operating policies or procedures of a particular affiliate with the specific purpose of facilitating such transactions.

Similar provisions relating to reexports by U.S. persons and U.S. person facilitation were incorporated into the Sudan Sanctions Regulations issued in 1997, with further explanation in part. While other OFAC sanctions regimes do not contain explicit prohibitions against facilitation, OFAC has interpreted virtually all of its other sanctions regimes to include such a prohibition.

10. The International Traffic in Arms Regulations.

In addition to the controls imposed on exports by the EAR, exporting companies must be aware of the International Traffic in Arms Regulations ("ITAR"), which govern certain electronics systems and electronics, spacecraft systems and associated equipment, including satellites, as well as other commodities more traditionally thought of as "arms", and specially designed parts and components of any of the foregoing. Consequently, exporters should consult the ITAR and the EAR to determine which regime controls their products.

The ITAR covers technical data as well as commodities. However, there are important differences between EAR and ITAR controls and licensing procedures. For example, a company that plans to provide defense services (*e.g.,* technical assistance, such as training or collaboration on a project) to a foreign entity first must submit an agreement for approval. This section discusses the types of commodities controlled by the ITAR, the licensing requirements for both equipment and technical data, exceptions to licensing, and special licensing requirements for defense services.

10.1. Scope of the ITAR.

The U.S. Munitions List ("Munitions List") (ITAR Part 121) sets forth the kinds of products, software, technology, and services subject to ITAR export control jurisdiction. The Munitions List names specific "defense articles," "defense services," and "technical data" related to defense articles and services. The Munitions List includes items that have no clear military applications – such as certain near-infrared cameras used in semiconductor manufacturing – and related services and technical data. In addition, the ITAR regulates registration of defense article manufacturers and exporters, licensing of Munitions List exports and imports, and penalties for violations.

10.2. Basic Export Determinations.

For each export transaction involving Munitions List items or technology, the basic determinations to be made are as follows:

(a) Is an ITAR exemption from licensing requirements applicable? If so, certify the applicability of the exemption and follow the proper export clearance procedures to document the shipment or other release or disclosure of technical data.

 bflowe@bcr-dc.com

(b) If the item is not otherwise exempt, determine whether to obtain DDTC approval of (i) an export license, (ii) a manufacturing license agreement ("MLA"), technical assistance agreement ("TAA"), or a distribution agreement, or (iii) an amendment to any such pre-existing authorization. Upon approval, follow proper export clearance procedures to document the shipment.

The ITAR requires that both exempt and licensed shipments follow specified export clearance procedures and that accurate records be maintained. Finally, exporters must ensure that their shipments adhere to all conditions of applicable licenses and exemptions.

10.3. Items Subject to ITAR Licensing Requirements.

10.3.1. Munitions List Articles. DDTC designates items for inclusion on the Munitions List when the article, service, or technical data: (1) is specifically designed, developed, configured, adapted, or modified for military application; (2) does not have predominantly civil applications; and (3) does not have performance equivalent (defined by form, fit and function) to those of an article or service used for civil applications; or (4) is specially designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability warranting its control. Items on the Munitions List can change occasionally as a result of the Commodity Jurisdiction Request process discussed in 10.3.5 below and also from reviews of the Munitions List that are intended to modernize the List. (Presently, one such review is ongoing as part of the Obama Administration's Export Control Reform Initiative "ECR Initiative".)

The Munitions List consists of 21 categories of defense articles, services, and technical data (22 C.F.R. Part 121). These categories are:

I	Firearms
II	Guns and Armament
III	Ammunition/Ordinance
IV	Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
V	Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
VI	Vessels of War and Special Naval Equipment
VII	Tanks and Military Vehicles
VIII	Aircraft and Associated Equipment
IX	Military Training Equipment and Training
X	Protective Personnel Equipment and Shelters
XI	Military Electronics
XII	Fire Control, Range Finder, Optical and Guidance and Control Equipment
XIII	Auxiliary Military Equipment (for example, military cryptographic devices, equipment incorporating particle beam technology, and so on)
XIV	Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
XV	Spacecraft Systems and Associated Equipment
XVI	Nuclear Weapons, Design and Testing Related Items
XVII	Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated

 bflowe@bcr-dc.com

XVIII Directed Energy Weapons
XIX [Reserved]
XX Submersible Vessels, Oceanographic and Associated Equipment
XXI Miscellaneous Articles (with substantial military applicability and specifically designed or modified for military purposes)

The ECR Initiative that is currently underway is making changes to these categories (e.g., a new Category XIX will cover military engines previously classified in other categories), and the items contains therein. The ECR Initiative is covered in substantial detail in Section 13.1 below.

10.3.2. Technical Data. The Munitions List controls "technical data" related to the listed defense articles. The ITAR defines technical data generally as: (1) information required for design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles; (2) classified information related to defense articles and services; (3) information covered by an invention secrecy order; and (4) software directly related to defense articles (ITAR §120.10). The definition includes, for example, information in the form of blueprints, drawings, photographs, plans, instructions, computer software, and documentation. It also includes information that enhances articles on the Munitions List.

Certain types of information do not rise to the level of technical data subject to ITAR control, including: (1) general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities; (2) other information in the public domain; and (3) basic marketing information on function, purpose, or general system descriptions of defense articles. The exclusion of such information from the definition of technical data allows a certain degree of information exchange for basic research and sales activities without obtaining a license.

The ITAR defines information in the public domain as that which is published and generally accessible or available to the public (ITAR §120.11). Examples of public domain information include publications available at book stands and libraries, materials freely distributed at U.S. trade shows, patents on file at a patent office, and fundamental research at U.S. universities.

If the information satisfies the definition of "technical data," exports of the information require a license from DDTC. Because of the nature of "technical data," an "export" can occur under a number of circumstances without the physical export of paper or software. For example, disclosure of technical data to a foreign national in the United States or a fax, internet, or modem transmission to a foreign country constitutes an "export" of "technical data", as does transfer of technical data outside the United States, even within the same country.

10.3.3. Software. The ITAR controls the export of software that is directly related to defense articles (ITAR §120.10(4)). Examples of software include: (1) system functional design; (2) logic flow; (3) algorithms; (4) applications programs; (5) operating systems; (6) support software for design, implementation, test, operation, diagnosis; and (7) repair.

Exports of controlled software require an export license. Software that is specifically named on the Munitions List is subject to the same licensing requirements as defense articles. To export other software, a technical data license is required.

 bflowe@bcr-dc.com

10.3.4. Defense Services. "Defense service" is currently defined as the furnishing of assistance to foreign persons in the "design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles" (ITAR §120.9). Providing defense services to a foreign person or foreign entity, even within the United States, requires approval by DDTC either in the form of an MLA or TAA. The furnishing of controlled technical data is also considered to be "defense services." U.S. persons may provide defense services even if all of the information that they are providing is not subject to the ITAR (*e.g.,* data that is in the public domain). As part of the ECR Initiative, on May 24, 2013, DDTC published a proposed rule that substantially revised the definition of "defense services." For more detail, see Section 13.3.12 below.

10.3.5. Commodity Jurisdiction Process. Whenever possible, the exporter should determine which set of regulations, ITAR or EAR, controls the export of particular products and technology. DDTC and BIS representatives work with company officials to determine conclusively which set of regulations govern. If there is any question as to whether the product is controlled by the ITAR's Munitions List or the EAR's Commerce Control List, the exporter should consider filing a "Commodity Jurisdiction Request" with DDTC, with a copy to BIS, to obtain a formal determination. Generally, exporters prefer their products to be within the jurisdiction of the EAR because its controls typically are less stringent than those of the ITAR, for example export under an EAR License Exception with no wait versus several weeks and sometimes months for an ITAR license application to be approved.

10.4. DDTC Registration.

All U.S. exporters, manufacturers, and brokers of "defense articles" must register with DDTC and pay annual registration fees (ITAR Part 122). Currently, foreign person brokers must also register with DDTC if they are located in the United States or are "otherwise subject to the jurisdiction of the United States" (ITAR §129.3(a)). DDTC interprets this to cover foreign persons, wherever located, that broker U.S.-origin defense articles. On August 26, 2013, DDTC issued an interim final rule that amends broker registration requirements. These amendments will become effective on October 25, 2013. For more detail on the new brokering regulations, see Section 13.5 below.

10.4.1. Who Must Register. Many U.S. manufacturers of defense articles do not realize they are required to register until they begin to export. This is particularly true for manufacturers of items considered to be primarily commercial, rather than military, in nature. DDTC traditionally has waived penalties for late registration if a manufacturer registers and applies for a license before exporting. Manufacturers rely on continuance of this lenient tradition at their peril. Registration does not confer a right to export, but is a prerequisite to obtaining most licenses.

10.4.2. Registration Process. To register, an exporter or manufacturer begins by preparing a Registration Statement for DDTC. The registration form must be accompanied by a transmittal letter certifying that the applicant company's officers and members of the board have not been indicted or convicted of violating U.S. criminal statutes and are not ineligible to contract with the U.S. Government or to receive an import or export license. The transmittal letter must also state whether the applicant is foreign owned or controlled. (Foreign ownership means that more than 50% of the voting stock is owned by foreign persons (that is, individuals or enti-

ties). Foreign control exists when foreign persons have control over the general policies or day-to-day operations of the applicant. It is presumed to exist when foreign parties own 25% or more of the voting stock and there is no offsetting U.S. ownership.) In addition to the transmittal letter, the registration application must include a certificate of incorporation (or other authorization to do business in the United States) and a receipt for electronic payment of the applicable registration fee.

DDTC assigns each registered exporter or manufacturer a "PM/DTC" registration number. Each of the registered exporter's subsidiaries and/or operating divisions should submit export license applications, referencing the PM/DTC number, in the name of the registered exporter with the division's company name and address listed in parenthesis under the registered exporter's name. The PM/DTC number should be referenced on all correspondence with DDTC.

It is essential that registered parties calendar the expiration of the registration to avoid a lapse in registration. Registrants must reapply for registration at least 30 days prior to the expiration date.

10.4.3. Updating the ITAR Registration. Many U.S. manufacturers and exporters overlook the need to file with DDTC timely updates to their registrations. The registered exporter or manufacturer is required to advise DDTC by registered mail within five days of any material changes to the Registration Statement (ITAR §122.4). DDTC requires a change notification when: (a) any of the senior officers or directors of the registered exporter listed in the Registration Statement (i) is indicted for or convicted of violating any of the U.S. criminal statutes listed in ITAR §120.27, or (ii) becomes ineligible to contract with, or to receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from, any U.S. government agency; or (b) there are any other material change in the information contained in the Registration Statement, such as the following: (1) a change in the senior officers listed therein, (2) the establishment, acquisition, or divestiture of a subsidiary or foreign affiliate, (3) a merger, (4) a change of location of the company headquarters or principal office of any of its operating divisions, or (5) dealing in an additional Munitions List category not listed in the Registration Statement.

Registered companies must also notify DDTC at least 60 days in advance of any intended sale or transfer to a foreign person of ownership or control of the company or any entity of the company (ITAR §122.4(b)). This required notice is in addition to the notices required by the Treasury Department-chaired Committee on Foreign Investment in the United States ("CFIUS") (31 C.F.R. Part 850).

Clearance by CFIUS avoids the potential that the President may block or order divestiture of an acquisition determined to jeopardize U.S. national security. The ITAR review is one substantive regulatory hurdle for foreign acquisitions that CFIUS considers. Companies negotiating a sale of assets or stock to a non-U.S. company must also make sure to obtain technical data licenses to cover any technological "exports" that may be required for the potential foreign investor's due diligence prior to the proposed acquisition.

If control of the registered exporter or manufacturer or any intervening parent company should change hands to another U.S. company, the registrant should discuss with DDTC whether an update to registration should be filed. It is prudent to do so even in a stock acquisition. An asset purchase will require the new company to register (if it has not already

 bflowe@bcr-dc.com

done so) and request amendment of existing ITAR authorizations due to a name and/or registration code change.

10.5. Restrictions on Technology Transfer.

Understanding the export controls over technical data is important to every company's export compliance program. However, because these controls are broad and nebulous, many exporting companies are unaware of the extent of these controls. Often, engineers and marketing personnel do not realize they may be exporting technical data when, for example, they escort a foreign engineer through a plant tour or discuss with foreign persons how well a military product works.

10.5.1. Licensing Requirements. Licenses are required for exports of ITAR-controlled technical data from the United States regardless of the origin of the technology. Although unaltered foreign-origin technology can be returned to the original source, its export to any other person requires a license. Even a return of the technical data to the original source will also require a license if the technical data has been enhanced or otherwise altered in any way unless the alterations are solely editorial and do not add to the technological content.

10.5.2. Exemptions. Technical data that is wholly within the public domain or that is covered by any of the following summary list of exemptions does not require an export license, except when exported to proscribed destinations (ITAR §125.4). The exemptions are set forth in ITAR §§ 125.4(b) & (c). The exemptions in ITAR § 125.4(b) cover technical data: (a) to be disclosed pursuant to an official written DoD directive or request; (b) in furtherance of an DDTC-approved MLA or TAA; (c) in furtherance of a contract between the company and a U.S. agency that specifically provides for the export, except for design, development, production, or manufacturing technology; (d) previously authorized for export to the same recipient in the exact same form, or with solely editorial revisions that do not add to the content of the technology; (e) basic operations, maintenance, and training information relating to equipment for which the company has an export license; (f) related to small firearms; (g) returned to the original source of import in the same, unaltered form; (h) directly related to classified data licensed for export to the same recipient, except for design, development, production, or manufacturing technology; (i) sent to a U.S. person employee of the company or to a U.S. government agency solely for their own use overseas; (j) exported by institutes of higher learning under specified conditions; (k) for which the company, pursuant to an arrangement with the Defense or Energy Departments, or NASA that requires such exports, has been granted an exemption in writing by DDTC (rare); (l) that is exempt under ITAR Part 126; or (m) that is approved for public release by the cognizant U.S. government department or agency in any form.

An exporter using any of these exemptions must abide by the specific requirements and conditions of the exemption. Shipping documentation for exempt physical technical data must include the exporter's certification of the applicable exemption.

ITAR § 125.4(c) was added to facilitate teaming or cooperation between U.S. and foreign companies in bidding on U.S. defense contracts. (65 *Fed. Reg.* 45282 (Jul. 21, 2000).) Under this provision, defense services and related unclassified technical data are exempt from licensing requirements so long as they are being exported to nationals of NATO countries, Japan, Sweden or Australia for the purposes of responding to a written request from the U.S. Defense Department for a quote or proposal. The defense services and technical data eligible for the

exemption are limited to the following types: "build-to-print", "build/design-to-specification", and "basic research". Ineligible services and data are "design methodology", "engineering analysis", and "manufacturing know-how". Definitions or explanations of these 6 terms are set forth in ITAR § 125.4(c)(1)-(6).

The exemption cannot be used for foreign production purposes. Therefore, if a U.S./foreign team is awarded a contract, a MLA (or a license in certain circumstances) must be obtained from DDTC before any additional defense services or technical data are furnished in furtherance of the contract.

For a brief description of the exemption for services provided under a Foreign Military Sales ("FMS") Program, see 10.6.1.2.

10.5.3. Obtaining Licenses for Technology Transfers. Any export of technical data related to defense articles or defense services that is not exempt will require an export license from DDTC (ITAR §125). An exporter must use Form DSP-5 for permanent exports of unclassified data, Form DSP-73 for temporary exports of unclassified data, or Form DSP-85 for any exports of classified technical data. These applications must be accompanied by the same documents listed below for equipment licenses, and are processed in the same manner. A reexporter from outside the United States would submit a letter of request rather than a license application form, and said letter would request authorization to reexport or retransfer the applicable items. It should contain the same information as an application form and would be subject to the same documentation requirements. DDTC refers to a request to reexport/retransfer as a "General Correspondence Case". The non-U.S. company may submit the request via the U.S. supplier or may do so directly if it wishes to have greater control or not involve the U.S. supplier. (ITAR § 123.9(c).)

10.5.4. Technical Assistance, Manufacturing License, and Distribution Agreements to Cover Programs Involving Technology Transfers. These agreements are simply ITAR authorizations that cover common commercial arrangements, such as teaming, licensing, joint venture, distribution, and other types of arrangements that also contemplate exports of ITAR-controlled technology or defense services as described below (ITAR §124.1). The agreements are between the U.S. and foreign parties and set forth the details of the technical data to be transferred and the agreement of the foreign party to comply with the ITAR, among other things. Agreements must be submitted in draft form and approved by DDTC before they can go into effect. Moreover, the ITAR prescribes certain clauses that must be included in such agreements, and some agreements are subject to congressional notification.

If exports of technical data are covered by an MLA or TAA approved in writing by DDTC, the export may be made without the requirement of any further licensing from DDTC (*i.e.*, in the form of a DSP-5, DSP-73 or DSP-85). The exporter must certify in the U.S. Census Automated Export System that the physically exported technical data does not exceed the scope of the agreement (ITAR §§124.3, 125.4(b)(2)). Such exports are authorized throughout the life of the agreement. These exports are eligible for an exemption because they have already effectively been licensed under the approved agreement. Consequently, whenever an exporter contemplates a program that will involve regular transfers of technical data to the same non-U.S. persons, that exporter should consider applying for an MLA or TAA. These approved agreements provide broader export authority and can eliminate the need to apply for licenses for each individual technical data transfer.

10.5.4.1. Manufacturing License Agreements. Under an MLA, a U.S. person authorizes a foreign person to manufacture or produce defense articles abroad. An MLA generally contemplates exports of technical data or defense articles or performance of defense services, or the use by foreign persons of technical data or defense articles previously exported. DDTC will at times authorize exports of products as well as technology under an MLA, but only if the MLA sets forth precise quantities, values, and specifications for hardware to be exported. Exporters often find it easier to cover such hardware exports under separate validated licenses.

10.5.4.2. Technical Assistance Agreements. A TAA is a contract for the performance of defense services or the disclosure of technical data only, but not for overseas manufacturing. It is frequently used in the context of research and development projects and sales where in-depth technical discussions are required. In addition, a TAA will be required for training of foreign persons in the design, engineering, operation, repair, or maintenance or defense articles on the Munitions List. Certain services can be provided under two noteworthy exemptions in ITAR § 124.2. ITAR § 124.2(a) authorizes basic operation and maintenance training to be provided for defense articles lawfully exported or authorized for export to the recipient of such training. This exemption does not authorize furnishing basic training for longer than two months in duration or that involves intermediate or depot level maintenance or higher level training.

An exemption in ITAR § 124.2(c) allows U.S. persons to provide maintenance services overseas with respect to unclassified U.S.-origin defense articles. (65 *Fed. Reg.* 45282 (Jul. 21, 2000).) The exemption is subject to important limitations. First, the defense services must be for defense articles lawfully exported or authorized for export, and owned or operated by, and in the inventory of, NATO or a NATO member state government, or the governments of Australia, Japan or Sweden. Second, the exemption does not apply to any transaction requiring congressional notification. Third, services provided must be limited to inspection, testing, calibration or repair. Excluded from the exemption are any modifications, enhancements, upgrades, or other alterations or improvements that enhance the performance or capability of the defense article. Fourth, supporting technical data must be unclassified and not include the types of software documentation identified in ITAR § 124.2(c)(4). Fifth, the exemption is not available for maintenance services for many Munitions List items, as set forth in ITAR § 124.2(c)(5).

If neither of these exemptions is available, then a TAA is required.

10.5.4.3. Required Information and Clauses for MLAs, TAAs, and Distribution Agreements. All proposed MLAs and TAAs must describe in detail: (a) the technology and equipment involved; (b) the information and assistance to be furnished; (c) the duration of the agreement; and (d) the country to which the transfer is to be licensed. (ITAR §§124.7, 124.8). Distribution Agreements require items (a), (c) and (d) of the above information. In addition, a Distribution Agreement must provide the terms and conditions of the export and distribution (ITAR §124.14(b)).

DDTC requires that all agreements contain certain clauses. The basic clauses are the same, but MLAs, and Distribution Agreements must contain certain additional clauses (ITAR §§124.9, 124.10, 124.14(c) and (d), 124.15(c)). These clauses are mandatory and virtually non-negotiable. DDTC will not approve such an agreement without these clauses or for which the company has modified the mandatory clauses, unless a very strong case is made for an

exception.

A straight sales contract for products without technical assistance or other services to be provided by the U.S. company is not legally required to be approved by DDTC or to contain such clauses (although a license will be required to export the products). Nevertheless, contingency or *force majeure* clauses are useful to include in sales contracts or agreements for the export of Munitions List items. Particularly in the case of sensitive equipment or destinations, the sales contract should contain a clause to protect the company from liability in the event of licensing delays or denial of the license. The clause should notify the foreign customer about U.S. export restrictions and indicate clearly that the company will not transfer any ITAR-controlled technology or products until it obtains appropriate export licenses.

10.5.4.4. Distribution Agreements. By submitting a "Distribution Agreement" for DDTC approval, a U.S. exporter can obtain approval to export defense articles to warehouses and distribution points outside of the United States (ITAR §124.14). This allows the exporter to ship articles during the duration of the agreement without having to obtain a license for each individual export. A Distribution Agreement is an agreement between the foreign distributor and the U.S. exporter. The agreement must specify the distribution territory to be approved.

Distribution Agreements, like MLAs and TAAs, function in place of individual licenses. And as with MLAs, parties to a Distribution Agreement must report to DDTC on an annual basis regarding the quantity, type, value, and purchaser of all articles shipped under the Agreement.

10.5.4.5. Obtaining DDTC Approval of Draft Agreements. Every agreement filed for approval with DDTC must be accompanied by a transmittal letter and certification. The transmittal and certification must contain the information and clauses required by the ITAR (ITAR §§124.12, 126.13). If the agreement relates to SME, classified articles, or classified data, a Form DSP-83 Nontransfer and Use Certificate signed by the foreign party must also be provided to DDTC. For classified articles or technology, the Form DSP-83 also must be signed by an authorized representative of the foreign government.

The approval process for agreements is similar to that for other DDTC licenses. Applicants should anticipate a *minimum* approval time of 60 days under current conditions. Depending on the complexity or sensitivity of the transaction, the review process may require more time.

10.5.4.6. Adherence to Conditions. Every agreement approved by DDTC will be subject to certain conditions, called provisos. These conditions may, for example, limit the scope of the services or technology to be provided (such as "no source code software is to be provided"). Amendments to an agreement must also be approved by DDTC before they can enter into force. Minor amendments that merely change delivery or performance terms or other minor administrative terms and do not alter the duration or scope of the agreement or any of the required clauses do not have to be approved by DDTC, but they must be transmitted to DDTC after execution.

Exporters generally find it helpful for the export administrator to provide a memo to company personnel who are implementing the approved agreement that clearly specifies

what work is covered and what work is not, as well as other limitations imposed by the approved agreement (expiration dates, and so on).

10.5.5. Subjecting Non-U.S. Technology to U.S. Export Controls. Technical data and technology that originates in another country becomes subject to U.S. export controls when brought into the United States. Upon export from the United States, this technology or technical data will require a license unless an exemption applies (ITAR §125.4(b)(7)), or unless the exporter is returning the unchanged information to the original source. Editorial changes are allowed for data being returned to the source; but, if the technological content is altered, the exporter must obtain a license to return the altered version. Because the application of U.S. export controls to non-U.S. origin technology is not well understood by laymen, exporters should consider establishing a procedure that requires any acquired technical data or technology to be brought to the attention of the company export compliance manager.

10.5.6. Employment of Foreign Nationals. Transfers of technical data related to Munitions List items to a foreign national employee are considered permanent exports and require a license from DDTC unless an exemption applies (ITAR §125.2(c)). "Foreign nationals" are persons who are not citizens or lawful permanent residents (*i.e.*, "green card" holders) of the United States. Protected individuals (that is, refugees or persons admitted for temporary residence and intending to become a U.S. citizen) are not considered foreign nationals for this purpose.

10.5.7. Foreign National Visits. Exports of technical data can frequently occur in the context of visits by foreign nationals to company facilities. Because such a visit may occur on short notice, the company may not have sufficient time in which to obtain an export license. In such instances, the company must limit the substance of the visits to exempt technical data, such as information in the public domain. The export manager should instruct all personnel participating in the visit on what types of technical data can and cannot be disclosed.

Government sponsorship of foreign visits can reduce licensing requirements. If the company has obtained a U.S. government agency-sponsored visit authorization, the disclosure of unclassified technical data will be exempt. Thus, it is often useful to obtain the sponsorship of a U.S. government agency to allow more latitude for foreign national visits. Otherwise, if non-exempt technical data will be discussed or otherwise revealed during the course of the visit, an export license must be obtained.

10.6. Licensing of Equipment Exports and Temporary (In-transit) Imports.

10.6.1. Exemptions to Licensing Requirements. Once the exporter has determined whether the items to be exported are ITAR-controlled , the exporter should consider whether any licensing exemptions apply.

10.6.1.1. Specific Exemptions. The ITAR provides certain exemptions from the requirement to obtain export licenses for equipment (ITAR §§123.16-123.20 and 126.4-126.5). Most notably, these exemptions are useful for those exporters planning to export: (1) hardware in furtherance of an approved MLA, TAA, or Distribution Agreement, but only if explicitly authorized by said agreement (see ITAR §123.16(b)(1)); (2) items on a temporary basis for trade shows, air shows, and public exhibitions (ITAR § 123.16(b)(4)); (3) components, parts, tools, or test equipment, on a temporary basis, to a subsidiary, affiliate, or facility owned or con-

 bflowe@bcr-dc.com

trolled by the registered U.S. exporter (ITAR §123.16(b)(9)); and (4) items by or for U.S. government agencies (ITAR §126.4).

Each of these licensing exemptions have different, often very technical requirements and export clearance instructions. If the exporter has a doubt as to whether an exemption would apply, the exporter should obtain a license rather than risk a violation.

10.6.1.2. Foreign Military Sales. Exports of defense articles and related defense services sold abroad under the Foreign Military Sales ("FMS") program are generally exempt from DDTC licensing requirements (ITAR §126.6). This exemption applies only to direct FMS sales of defense articles for export, which are sales contracts directly between the U.S. Government and a foreign entity. It does not apply to FMS credit financing by the U.S. Government of a private sale to a foreign entity. An FMS program sale of defense articles must be made pursuant to a U.S. Department of Defense Letter of Offer and Acceptance. To clear U.S. Customs without a license, a form DSP-94 must accompany FMS exports, and a copy of the Letter of Offer and Acceptance must accompany classified articles exported under the FMS program.

10.6.2. Export Applications and Filing. If an exporter has determined that no license exemption applies to the equipment to be exported, the exporter must apply for and obtain a license prior to shipping the equipment. It is essential that the exporter use the appropriate application form as described below (ITAR §123.1(a)).

Unclassified Articles:

DSP-5 – permanent exports

DSP-73 – temporary exports

DSP-61 – in-transit shipment (covering the temporary import into the U.S. and subsequent to a third country or the country of origin).

Classified Articles:

DSP-85 – permanent and temporary exports and temporary imports (classified equipment and technical data).

Each block on the license application must be completed, and the license application must be signed by an "empowered official" of the company. Exporters must submit license applications to DDTC electronically through DDTC's D-Trade system.

As with technical data, discussed in 10.5.3, authorization for reexport or retransfer of hardware is requested by submitting a letter of request containing the same information that would be in an application form and including the same support documentation. This is referred to as a "General Correspondence Case" and may be submitted by the non-U.S. company directly or by the U.S. supplier. (ITAR § 123.9(c).)

10.6.3. Accompanying Documents. Exporters must include with the license application the following documents (ITAR §123.1(c)): (1) purchase order or letter of intent,

 bflowe@bcr-dc.com

signed by the foreign customer, for permanent exports only; (2) Form DSP-83 "Non-Transfer and Use Certificate" executed by the foreign customer for classified equipment and for SME; (3) ITAR § 126.13(a) certification for agreements; (4) list of all U.S. consignors and freight forwarders, and of all foreign consignees and foreign intermediate consignees that should include the names and telephone numbers of contact persons for all foreign consignees; (5) literature describing the equipment in sufficient detail to enable the DDTC Licensing Officer and other agency representatives reviewing the case to understand thoroughly the subject of the license application; and (6) political contribution, fees, and commissions statement for exports valued at $500,000 or more. Exporters must submit to DDTC the application and supporting documentation through DDTC's D-Trade online license application platform.

10.6.4. Certifications. All license applications, MLAs, TAAs, and other requests for export authorization require an ITAR §126.13 certification. This must contain certifications for the following facts regarding the applicant: (1) neither the applicant nor its officers or directors has been indicted or convicted of violating certain enumerated federal criminal statutes (ITAR §120.27); (2) neither the applicant nor its officers or directors is ineligible to contract with, or receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from, any U.S. government agency; (3) to the best of the applicant's knowledge, no party to the export is the subject of any of the conditions listed in (1) and (2) above (including freight forwarders, exporting agents, consignees, and end-users) (ITAR §126.7(e)); and (4) the natural person signing the license application or other request is a U.S. citizen, or has been lawfully admitted to the United States for permanent residence and maintains a residence in the United States.

10.6.5. Empowered Officials Required to Sign. The certification, like the application, must be signed by a responsible official empowered by the applicant. An "empowered official" is a company official who meets the following requirements: (1) is directly employed by the applicant or its subsidiary, and has authority for policy or management; (2) is legally empowered in writing to sign license applications on behalf of the applicant; (3) understands the provisions of the ITAR and the Arms Export Control Act as well as the liability for violations of these laws; and (4) has independent authority to inquire into an export, verify its legality, and refuse to sign a license application or other request without adverse consequences. Typical examples of officials that may qualify as empowered officials include a general counsel, vice president for finance, traffic manager, or export compliance manager.

10.6.6. Licensing Process. From start to finish, DDTC's goal is to complete review of export license applications within 60 days. The Department of Defense (DoD) and other reviewing agencies officially have 30 days to review a case and return their recommendations to DDTC. However, these time limits are prescribed by internal agency agreements rather than by law and so are not always strictly adhered to. Approval of licenses often requires considerably more time. This is especially true if the application is controversial. Accordingly, exporters should apply for licenses *at least* 90 days (90 - 180 days for agreements) in advance of the expected ship date or date for commencement of work under an agreement for unclassified products and technology, and 120-150 days for classified items.

Exporters should prepare the applications carefully to provide reviewing officials all essential information on the products, technology or services, the intended end-use, a history of precedent cases for the same or similar products (with copies of licenses as appropriate), foreign competition for the sale, and other data to help speed their review. Because the approval

process can still be lengthy, it is important for the exporter to monitor the case at each step of the proceedings to press for approval of their case at appropriate times and places.

10.6.7. Proscribed Countries: Licensing Policy. Before deciding to market or export Munitions List items to any particular country, the exporter should consult the list of proscribed destinations. Subject to a few narrow exceptions, the U.S. Government maintains a policy of generally denying export licenses to these destinations (ITAR §126.1). This policy extends to the embassies or consulates of these countries and vessels and aircraft owned or operated by or leased to or from any such countries. None of the ITAR exemptions applies to exports to such countries. An exporter must obtain the specific approval of DDTC before attempting to make a proposal to sell or transfer any defense articles, services or technology to such countries.

The current list of proscribed destinations is as follows:

- Afghanistan
- Belarus
- Burma/Myanmar
- China (PRC)
- Côte d'Ivoire
- Cuba
- Cyprus
- Democratic Republic of Congo
- Eritrea
- Fiji
- Haiti
- Iran
- Iraq
- Lebanon
- Liberia
- Libya
- North Korea
- Somalia
- Sri Lanka
- Republic of Sudan
- Syria
- Venezuela
- Vietnam
- Zimbabwe

This list of countries was static for many years, but recently countries have been added or deleted fairly often, reflecting geopolitical changes. DDTC periodically announces new country policies in the *Federal Register*.

On rare occasions, as noted above, DDTC may make an exception to the general policy of denial. DDTC generally requires a presidential waiver to make such an exception. Because of the great likelihood of denial by DDTC, business opportunities in these countries require careful consideration.

 bflowe@bcr-dc.com

10.6.8. Temporary (In-transit) Imports. An exporter must obtain a license for temporary import (also known as in-transit shipment) of Munitions List items. Temporary imports may arise in two different situations: (1) defense articles which are imported into the United States temporarily and which will be returned to the country that exported the articles, or (2) unclassified defense articles which are temporarily imported in transit to a third country.

Form DSP-61 is the proper application form to submit for temporary (in-transit) import licenses for unclassified items (ITAR §123.3). Under certain circumstances, unclassified items may be eligible for a licensing exemption, including importations for servicing or exhibition. Temporary importations of classified articles require a Form DSP-85 license application (ITAR §125.7). The DDTC temporary (in-transit) import license will authorize both the U.S. import and subsequent U.S. export as set forth on the license. Both types of applications must be accompanied by the same supporting documents described above for equipment licenses, except that a purchase order or letter of intent is only required for items to be reshipped to a third country.

10.7. Comprehensive Authorizations for Exports of Equipment and Technology.

In a final rule issued on July 21, 2000, the State Department amended the ITAR to create four comprehensive licensing mechanisms for exports and reexports of defense items to NATO countries,[9] Australia, Japan, and Sweden. (65 *Fed. Reg.* 45282 (Jul. 21, 2000).)

The four comprehensive licenses are the Major Project Authorization, the Major Program Authorization, the Global Project Authorization, and the Technical Data Supporting an Acquisition, Teaming Arrangement, Merger, Joint Venture Authorization. The authorizations may be utilized under "circumstances where the full parameters of a commercial export endeavor including the needed defense exports can be well anticipated and described in advance, thereby making use of such comprehensive authorizations appropriate". (ITAR § 126.14(a).) Even with the regulation, the authorizations remain somewhat vague. Only one, a Global Project Authorization for the Joint Strike Fighter Program, has been approved by DDTC to date and it has not been used by the parties supposedly due to questions over the liability of the prime contractor and certain restrictive provisos placed on the arrangement. Hopefully, the Obama ECR Initiative will breathe some new life into these provisions.

Exporters are not required to use the authorizations, although the authorizations offer, at least in theory, to provide exporters required licensing in a more expeditious and cost- effective manner than under the alternative licensing regime.

The main features of the authorizations are as follows:

10.7.1. Major Project Authorization. Created to facilitate the procurement of U.S. defense products by Allied Governments, this authorization is available to a registered U.S. exporter/prime contractor for the entire scope of a "major project". (ITAR § 126.14(a)(1).) A "major project" is a project that involves, for example, the "export of a major weapons system for

[9]In addition to the United States, NATO members include: Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, and the United Kingdom.

 bflowe@bcr-dc.com

a foreign government involving . . . multiple U.S. suppliers under a commercial teaming agreement to design, develop and manufacture defense articles to meet a foreign government's requirements." ITAR § 126.14(a)(1).

This authorization requires applicants to provide DDTC detailed information concerning the scope of the project, including foreign government end-users, other exporters, U.S. subcontractors, other participants, and planned defense exports.

In order to obtain the maximum benefit of the authorization, potential applicants for an authorization must carefully think through all aspects of the entire project for which the authorization will be sought before seeking the authorization. For all comprehensive authorizations, consideration might need to be given to applying for both comprehensive and narrow licenses in cases where an individual shipment in a large project is extremely time-sensitive and could be more quickly reviewed by U.S. government officials than a comprehensive license application.

10.7.2. Major Program Authorization. This authorization provides an umbrella under which a single registered U.S. exporter can make all exports needed with respect to a "major" program, including exports and reexports of hardware, technical data, defense services, development, manufacturing, and logistic support. (ITAR § 126.14(a)(2).) In fact, to be eligible for the authorization, the exporter must be offering to provide all phases of support for a "major" program. As with the major project license, an applicant must furnish DDTC detailed information about the program's scope, including all planned exports and reexports of defense items.

10.7.3. Global Project Authorization. This authorization permits registered U.S. exporters to export defense items in support of agreements (*e.g.*, Memoranda of Understanding ("MOU")) between the United States and governments of one or more of the NATO member states, Sweden, Japan, or Australia. (ITAR § 126.14(a)(3).)

After execution of such an agreement, the U.S. Defense Department will prepare a set of standard terms and conditions to apply to activities to be conducted under the agreement. The terms and conditions will provide the basis for the Global Project Authorization for U.S. exporters identified by Defense as project participants. The participants will be able to submit one single comprehensive application package, which can consist of a variety of types of license applications (*e.g.*, TAAs, DSP-5 applications to export unclassified defense items, etc.) covering specific transactions under the project.

Eligible end-users are limited to the defense ministries of the countries that are parties to the agreement with the United States and to foreign companies that are contractors for these countries. While such contractors will need to execute a DSP-83 (Nontransfer and Use Certificate), governments that are parties to the agreement with the United States are exempted from this documentation requirement so long as the agreement contains assurances comparable to those required by a DSP-83 with respect to foreign governments and provide that the government is undertaking responsibility for its participating companies.

This provision clarified an area of some confusion for U.S. exporters and foreign governments and their prime contractors. Foreign governments and their contractors (and some U.S. exporters) often had assumed that once an MOU was concluded, no DDTC licensing was required. Although under the provision DDTC licensing is required, even when exports and

reexport are made pursuant to an MOU, DDTC offered in the regulation to streamline the licensing process under this authorization.

10.7.4. Technical Data Supporting an Acquisition, Teaming Agreement, Merger, Joint Venture Authorization. This authorization permits registered U.S. defense companies to export technical data to "qualifying well established foreign defense firms", in eligible destinations, in connection with consideration by the U.S. exporter of entering into a teaming arrangement, joint venture, merger, acquisition, or similar arrangement with such foreign firms. (ITAR § 126.14(a)(4).) The ITAR does not define the term "qualifying well established foreign defense firm". Applicants for the authorization must provide detailed information to DDTC regarding the possible arrangement and any planned exports of defense items.

10.7.5. Application and Other Requirements Governing All Four Comprehensive Authorizations. To apply for a comprehensive authorization, exporters should send a letter to DDTC with the following information:

(1) description of proposed program or project, including where appropriate a comprehensive description of all phases or stages;
(2) value of the proposed program or project;
(3) types of exports and reexports;
(4) projected duration of program or project, subject to a 10 year limitation;
(5) description of exporter's plan for recordkeeping and auditing of all phases of the program or project; and
(6) identification of the project (in case of exports in support of government-to-government agreements).

The regulations provide that exporters unsure about eligibility for an authorization may consult with DDTC. (ITAR § 126.14(b)). Amendments to authorizations may be requested. Apparently, extensions of authorizations can also be requested in the form of amendments.

Authorizations must comply with all applicable requirements of the ITAR. Some of these requirements are specifically listed in the rule as follows: Part 124 (e.g., §§ 124.7-9 (information and clauses required in TAAs and MLAs), § 125.4 (technical data exported in furtherance of an agreement), § 123.16 (hardware being included in an agreement), §§ 123.15 and 124.11 (congressional notification requirements), §§ 123.10 and 124.10 (non-transfer and use assurances), § 123.9, and §126.13.

Exporters are required to establish special auditing and reporting requirements to qualify for any of the authorizations. In particular, under ITAR § 126.14(b)(6), exporters must establish an electronic system for keeping records of defense exports made under the authorizations. This requirement applies to all holders of a comprehensive authorization. In addition to these special auditing and reporting requirements, it would be prudent for exporters to establish procedures to ensure compliance with the terms and limitations of any comprehensive authorizations that are granted.

10.8. Congressional Notification and Waiting Period.

Congressional Notification by DDTC and a 30-day waiting period are required before

 bflowe@bcr-dc.com

DDTC can grant a license for the following types of transactions (ITAR §§123.15, 124.11): (1) exports or third country transfers of "Major Defense Equipment" sold under a contract in the amount of $14 million or more; (2) contracts for the export of any defense articles or services valued at $50 million or more; and (3) MLAs or TAAs for production of SME in non-NATO countries.

In cases where NATO member countries, Australia, Japan, South Korea or New Zealand are the destinations, congressional notification by DDTC and a 15-day waiting period are required before DDTC can grant a license for: (1) transfers of "Major Defense Equipment" sold under a contract in the amount of $25 million or more or (2) contracts for the export of any defense articles or services valued at $100 million or more.

("Major defense equipment" is SME having a nonrecurring research and development cost of $50 million or more, or a total production cost of $200 million or more.)

The purpose of Congressional Notification is to give Congress an opportunity to enact a joint resolution prohibiting the export. Such a joint resolution must be approved by both the House and the Senate and signed by the President to prevent the transaction. To date, no such formal action has ever blocked a proposed approval of a defense export. However, concerns over Congressional review can and have influenced major sales of SME, which can carry with them the imprimatur of U.S. foreign policy to contribute to defense of certain countries, particularly in the Middle East.

Accordingly, exporters often lobby such sales carefully with members of the House Committee on Foreign Affairs and Senate Foreign Relations Committee, who receive DDTC's Congressional Notifications. Opponents of particular sales have also been known to raise concerns with congressional officials.

Even exports that are exempt from licensing must comply with the Congressional Notification requirement if the export meets the criteria for Congressional Notification described above. This circumstance may arise, for example, with respect to exports to Canada. The exporter must submit a letter to DDTC describing the proposed transaction, a signed contract, and a "Non-transfer and Use Certificate" (Form DSP-83). DDTC will transmit the matter to Congress, and the exporter must wait until the expiration of the 30-day period before proceeding with the export.

10.9. Political Contributions, Fees, and Commissions.

Commercial sales of defense articles or defense services valued at $500,000 or more, for use by the armed services of a foreign country, require a statement regarding political contributions, fees, and commissions (ITAR Part 130). The statement must confirm whether the applicant or its vendors or suppliers, either directly or indirectly, have paid or have offered or agreed to pay, in respect to any sale for which a license or other approval is requested: (1) political contributions in an aggregate amount of $5,000; or (2) fees or commissions in an aggregate amount of $100,000 or more.

If the applicant or its vendors or suppliers have made or offered to make payments exceeding these amounts, the applicant must provide information to DDTC on such payments, including: (1) the amount of each payment; (2) date of each payment; (3) recipient of each pay-

ment; (4) person who made each payment; and (5) aggregate amount of each payment.

Any party supplying this information to DDTC should identify all information in the report that is confidential commercial or financial information. The government and its employees are generally prohibited from disclosing confidential information by Section 38 of the Arms Export Control Act, ITAR §126.10, the Freedom of Information Act, and Trade Secrets Act (18 U.S.C. §1905).

Exporters should be aware that the Foreign Corrupt Practices Act ("FCPA") imposes criminal penalties for making certain payments, directly or indirectly, to foreign governmental officials. To date, the law does not require DDTC to provide copies of political contribution information to Justice Department officials who enforce the FCPA.

10.10. Shipment/Export Clearance and Brokering Activities.

10.10.1. Shipping– Export Clearance Requirements. For physical shipments made directly by the exporter under license, the exporter must: (1) deposit the original license with the District Director of Customs at the port of exit for endorsement (and Customs will return it to DDTC when the total value or quantity authorized has been shipped or when the expiration date has been reached); (2) electronically file with Customs using the Automated Export System; and (3) place an appropriate "destination control statement" on the waybill and the invoice accompanying the shipment (ITAR §123.22).

The following destination control statement shall be used for physical ITAR shipments (ITAR §123.9(b)):

> *These commodities are authorized by the U.S. Government for export only to [country of ultimate destination] for use by [end-user]. They may not be transferred, transhipped on a non-continuous voyage, or otherwise be disposed of in any other country, either in their original form or after being incorporated into other end-items, without the prior approval of the U.S. Department of State.*

Note that this destination control statement differs from that required under the EAR. Unless properly trained, exporters' shipping departments can mix up which destination control statement is required. A standard EAR statement is often printed on shipping documents.

These requirements do not apply to reexports, except for exports in furtherance of Distribution Agreements, but are used along with DSP-83 certifications and TAA and MLA provisions by U.S. enforcement authorities to assert personal jurisdiction on non-U.S. reexporters based on the notion that they have consented to such jurisdiction or at least have notice of it.

10.10.2. Brokering Activities. The ITAR also requires the registration with DDTC of persons engaged in the business of brokering activities with respect to the manufacture, export, import, or transfer of defense articles or defense services. (ITAR Part 129). The regulation also required that these brokering activities be authorized in advance by a license or other written approval from DDTC. The following is a description of the brokering regulations that exist today. However, on August 26, 2013, DDTC published an interim final rule that substantially amends the brokering regulations, which will go into effect on October 15, 2013. For more information on the amendments to the brokering regulations, see Section 13.5 below.

The brokering regulation represents a trap for the unwary since its broad and somewhat murky language may be susceptible to extremely broad interpretations by enforcement officials. ITAR § 129.2(a) defines the term "broker" as "any person who acts as an agent for others in negotiating or arranging contracts, purchases, sales or transfers of defense articles or defense services in return for a fee, commission, or other consideration." Under ITAR § 129.2(b), "[b]rokering activities means acting as a broker . . . and includes the financing, transportation, freight-forwarding, or taking of any other action that facilitates the manufacture, export, or import of a defense article or defense service, irrespective of its origin." These ITAR provisions could easily be interpreted to govern activities that are not typically viewed as brokering by industry.

Further, the jurisdictional reach of the regulation is sweeping, even by ITAR standards. Registration and licensing requirements apply to any U.S. individuals or entities, wherever located, engaged in brokering activities with respect to any U.S. or foreign defense articles or defense services. Foreign individuals or entities must comply with the brokering regulation if they are located in the United States or otherwise subject to U.S. jurisdiction. DDTC interprets this to cover foreign persons, wherever located, that broker U.S.-origin defense articles.

The brokering regulation has important exemptions. Activities by U.S. persons that are limited exclusively to U.S. domestic sales or transfers are not subject to the regulation's registration and licensing requirements. Financial institutions, freight forwarders, and transportation companies are exempted from the regulation's requirements so long as they are not directly involved in arranging arms deals and do not hold title to defense articles. Thus, registration is not required for banks that provide commercially available lines or letters of credit to registered arms exporters or for air carriers or freight forwarders that merely transport licensed U.S. Munitions List articles. A particularly notable exception to the brokering amendment's licensing requirements is provided in ITAR § 129.6(b)(2) for "[b]rokering activities that are arranged wholly within and destined exclusively for the North Atlantic Treaty Organization, any member country of that Organization, Israel, Japan, Australia, South Korea or New Zealand," except in cases involving certain sensitive defense articles or defense services.

Even persons already registered as arms manufacturers or exporters are affected by the brokering regulation. For example, under ITAR § 129.4(b), they must provide notification of their brokering activities to DDTC and pay an additional registration fee. As another example, they must provide 30 day advance written notification to DDTC of brokering proposals or presentations with respect to SME valued at less than $1,000,000. (ITAR § 129.8.) The sharing of basic marketing information is excepted from this notification requirement.

10.11. Limited Reexport Exemptions.

Unlike the EAR, the ITAR have very few exemptions for reexports. ITAR § 123.9(d) says that the written approval of DDTC must be obtained to resell, transfer, transship, or otherwise dispose of defense articles in any country other than what is authorized by the license, to anyone other than the end-user stated on the license, or to any end-use not authorized by the license. If the exemptions described above would apply to a U.S. export, we believe they would apply to a reexport, although DDTC officials have always avoided answering this question when it is put to them.

 bflowe@bcr-dc.com

10.11.1. Exemption for Retransfers of U.S. Components in Non-U.S. Made Items to NATO Governments. ITAR § 123.9(e) does authorize retransfers without prior written approval of U.S.-origin components incorporated into a non-U.S. made defense article but only to a government of a NATO country, Australia, New Zealand, South Korea or Japan, and only if (a) the items were authorized for export from the United States in the first place, (b) they are not SME, (c) they are not Major Defense Equipment sold under a Contract in the amount of $25 million or more, (d) they are not defense articles or services sold under a contract in the amount of $100 million or more; and (e) they are not identified as Missile Technology Control Regime items. The party taking advantage of this exemption must provide DDTC with written notification within 30 days of the export.

10.11.2. Seek Authorization Up Front. An ITAR License can authorize in advance a reexport to another end-user, and this should also be reflected on the Form DSP-83 End-User Certificate that you supply to support the license. However, simply indicating the end-user on the DSP-83 is not sufficient if the license itself does not authorize the reexport to that end-user. The license is controlling.

10.11.3. Reexports to the United States. Permanent imports into the United States of Munitions List articles are governed principally by the "Munitions Import List", a subset of the ITAR Munitions List, which is set forth in 27 C.F.R. Part 447 and administered by the Justice Department's Bureau of Alcohol, Tobacco, Firearms and Explosives ("BATF"), in consultation with the Departments of State and Defense. For example, most missile related products are covered by the Munitions Import List and require authorization to be imported back into the United States (in contrast with Categories IX through XIII, which do not apply to imports).

Temporary imports of defense articles into the United States are governed by DDTC under the ITAR. Most imports of such items are temporary ones and thus can best be covered by a Form DSP-61 temporary import authorization application to DDTC. An approved Form DSP-61 authorizes both the import into the United States and the subsequent reexport. It is not unusual for U.S. companies to find out for the first time that Customs is holding Munitions List imports being returned for repair, and the importer must quickly obtain the proper authorization. Many U.S. defense companies have as part of their return materials authorization requirements a procedure to ensure that appropriate licenses are obtained or exemptions used before the return shipments are initiated to the United States, but others do not. ITAR § 123.4(a), however, exempts the temporary import and subsequent export of U.S.-origin defense articles that are returned to the United States for service, upgrade, and marketing under certain conditions.

A. Returns Due to Quality Problems. As described above, the importer of record, which may be your company via a freight forwarder if not the original supplier, depending on how you complete your shipping documents, must qualify for an exemption or obtain the appropriate license from BATF or DDTC for Munitions Import List items before the item can clear U.S. Customs legally. Care must be taken, especially when using the temporary import exemptions in ITAR §123.4(a) to correctly mark the importation paperwork in accordance with the procedures set forth in the exemption in order to avoid complications with the subsequent export of goods returned due to quality problems. Also, it is important for the importer to complete paperwork correctly to avoid Customs duties on U.S. goods returned. I advise you to consult and coordinate with the U.S. supplier in advance to ensure that it can

legally import the items and so it can act as the importer of record, obtaining the required approvals.

B. Shipments to U.S. Customers. Shipments to U.S. companies will require appropriate authorization as described above. Imports by U.S. agencies and imports of components of items being manufactured under contract for the Department of Defense ("DoD") are exempt from BATF import authorization requirements, but the importer must present to Customs with the shipment satisfactory proof that the applicable exemption is met (*e.g.*, a letter from DoD or State). 27 C.F.R. § 47.53. There are no specific exemptions for shipments to the embassies or military departments of foreign countries.

C. Temporary Imports. As a legal matter, and as a general rule, if a company is not the importer of record, you need not check to determine if the importer has the requisite license unless you have reason to know that it does not. As a practical matter, it is always better to ask the question first. Having Customs seize or even just detain imported goods costs everyone involved time and money.

10.11.4. *De Minimis* Rule Applies Only to EAR Items. The *de minimis* rule is a rule under the EAR. Thus, items otherwise "subject to the EAR" are no longer "subject to the EAR" if they are incorporated as parts and components of items outside the United States and amount to less than 10% of the end-item. The EAR only lists a few items to which the *de minimis* rule does not apply (certain high performance computers, "Encryption Items", and certain satellites). None of the listed exceptions cover other "defense articles". The ITAR does not contain any *de minimis* rule. Thus, if one imports U.S. defense articles under the ITAR under license or other authorization, there is no specific authority under the ITAR to incorporate them into your defense articles and reexport them. Such U.S. legal authority must be found by license or other authorization issued by the DDTC or under a license exception under the ITAR. This is a difference between the ITAR and the EAR. And, items covered by the ITAR are not "subject to the EAR", so the EAR *de minimis* rule does not apply to U.S. exported "defense articles".

The hard question is what rules apply to EAR covered U.S.-origin items that a non-U.S. company uses as components of non-U.S.-made defense articles (such as integrated circuits or basic hardware incorporated into a missile). My view is that such items would not be subject to U.S. export controls if they amount to less than 10% of the end product and otherwise meet the EAR *de minimis* rule requirements. The ITAR would have no jurisdiction because the items exported from the United States were not subject to the ITAR. However, I must caution that this question has not been thoroughly considered by U.S. export control officials. It is quite conceivable that DDTC officials would take a different position, regardless of whether it is defensible (or whether anyone outside the United States adheres to such a position).

11. Enforcement Risks.

Exporters need to be aware of the significant enforcement risks attached to export activities. Each of the export control statutes provide significant penalties for export violations. These penalties include:

- fines of up to $1 million per violation (civil and criminal),

 bflowe@bcr-dc.com

- imprisonment, and
- loss of exporting privileges via denial orders (which can shut down a business).

Collateral penalties can be applied by other agencies, including debarment from the ability to contract with U.S. government agencies and, in some cases, prohibition against imports as well as exports.

As mentioned previously, the denial order is most frequently employed against non-U.S. companies because it is the only sanction that U.S. agencies can enforce effectively against most persons located outside the United States. Quite often, denial orders are imposed against non-U.S. companies who simply do not answer a "charging letter" from U.S. export enforcement officials or, if they do answer, do not request a "hearing". Failure to answer a "charging letter" from the Office of Export Enforcement of the Commerce Department or to request a hearing effectively waives the company's right to contest the matter and leaves the enforcement authorities free to impose whatever penalties they deem appropriate. Companies who let such deadlines go by almost always regret it. While no company likes to be assessed any level of penalty, U.S. officials generally settle contested enforcement cases with far more reasonable sanctions than those they impose on companies who do not respond or do not contest charges brought against them.

The public relations impact of being branded as a diverter of exports for purposes of greed that jeopardized security or created proliferation risks can devastate a business to an even greater extent than the formal penalties.

Many of the U.S. export control laws are "strict liability" laws. This means that, if any violation occurs, the exporter is liable regardless of whether anyone intentionally violated the law or simply did so unknowingly. The more severe penalties are based on "knowledge" that can be inferred from circumstances or various facts that certain employees know (but regarding which they may be unaware of the significance).

We have available on request a separate analysis on whether or not to submit voluntary disclosures of violations, what steps to take to cure systemic problems discovered and prevent others regardless, and if submitting, how best to present disclosures and behave to maximize chances for a warning letter and minimize risks of substantial fines or other penalties.

Each of DDTC, BIS, and OFAC publish all of their enforcement cases at the following links: DDTC http://www.pmddtc.state.gov/compliance/index.html, BIS http://efoia.bis.doc.gov/exportcontrolviolations/tocexportviolations.htm (all) and http://www.bis.doc.gov/complianceandenforcement/dontletthishappentoyou_2010.pdf (selected), OFAC http://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx. Most also have Department of Justice criminal violations.

Further discussion of enforcement is beyond the scope of this Guide, but it is far less costly to spend ounces to prevent violations, than pounds to defend them.

 bflowe@bcr-dc.com

12. Utility and Need for Compliance Programs.

Prudent exporters subject to U.S. export and reexport controls should develop export compliance programs to manage and minimize the risks of complex export controls and make compliance with the law more efficient as well as effective. A solid export compliance program with appropriate management support provides guidelines for customer and shipment screening, classifying products, and licensing. A compliance program establishes order processing and shipping controls to prevent violations. Training is an integral part of the program to ensure that personnel know what is involved. Employees directly involved in exports must appreciate the importance of export compliance procedures, and other employees need to learn to recognize an export transaction so that they can bring it to the attention of the export compliance staff. A good compliance program is essential to avoiding violations before they happen.

12.1. Reasons that an Export Compliance Program is Necessary and Useful.

Export compliance programs have not usually been a business priority unless a company has violated export controls laws and is negotiating for lesser penalties; has adopted a license under which such a program is required by law; or has discovered that the government seems likely to audit compliance and may find violations. However, compliance programs should be instituted before rather than after disaster strikes for the following reasons:

a. Mitigation of Penalties, both for Prior Violations and for Future Violations. High volume exporters are bound to have problems from time to time no matter how good their compliance program. In general, special provisions of the Federal Sentencing Guidelines allow corporations to reduce their exposure to liability and avoid harsh penalties if they have implemented good compliance programs. Likewise, recent court cases have stated that corporate directors may be personally liable if their company does not establish procedures to comply with certain laws. EAR Mitigation Guidelines in Supplements 1 and 2 to EAR Part 766 have stated that exporters are entitled to "great weight" (up to 25%) reduction in penalties in enforcement cases if they have an "effective compliance program." There has long been debate as to what those terms mean. Enforcement officials could always say, "if it were effective, we would not be discussing your violation," whereas exporters always want as much credit as possible. In a speech in Newport Beach in March 2008, then Assistant Secretary of Commerce for Export Enforcement Darryl Jackson announced some principals that BIS's Office of Export Enforcement had developed as to what constitutes an effective program deserving such mitigation. The speech, the presentation, and a design and implementation checklist (largely mirroring the discussion below) are now on the BIS Enforcement web site. http://www.bis.doc.gov/complianceandenforcement/index.htm

b. Compliance with Rules Mandating Compliance Programs. As a condition of eligibility for a Special Comprehensive License, the Holder and each of its Foreign Consignees must establish a formal Internal Compliance Program subject to audit by the Commerce Department. (EAR § 752.1(b).) Similarly, government agencies have at times agreed not to block a foreign acquisition of a U.S. business on national security grounds if the U.S. company established a formal export compliance program to ensure against unauthorized transfers of technology to the foreign parent or others. And, many settlements of enforcement cases are conditioned on the company adopting and enforcing a good compliance program.

c. Meeting Expectations of Government Export Control Officials and

 bflowe@bcr-dc.com

Preparation and Readiness for Government Audits. Most companies recognize they should maintain the essential elements of a Compliance Program, both to mollify government officials and to help ensure their compliance with the law. Restrictions on the use of License Exceptions and Recordkeeping requirements make up the essential elements of the Compliance Program. The importance of "knowledge"-based export controls on end-users and end-uses also highlights a need for companies to maintain compliance programs to avoid violations in making shipments under general licenses. The administrative elements of compliance programs simply make good sense to ensure legal and efficient compliance with the law. Although BIS changed its requirements for mandatory "Internal Compliance Programs" into "voluntary" "Export Management Systems", and more recently the "Export Management and Compliance Program" the elements are almost exactly the same. The State Department also has mandated formal compliance programs in recent enforcement cases, and OFAC strongly suggests them as well.

d. Ensuring Against Risks of Violations. U.S. and other export control laws are complex to apply, and they are not getting simpler. A comprehensive export compliance program helps a company understand and implement its responsibilities and reduces the likelihood of mistakes. Potential penalties for violation include denial of the privilege of exporting (which can shatter an international business), damaging publicity, as well as significant fines and jail time. By comparison, the expense of establishing an export compliance program is a wise investment akin to risk insurance premiums. Generally, outside counsel and consultants earn five to ten times more defending a single company that has violated the law than they will in helping to establish strong programs in several companies for avoiding violations.

e. Making Compliance and thus Exporting More Efficient. An organized system of compliance helps speed decisions concerning whether specific licenses or licenses are required and how to apply for and obtain them in a timely fashion. Today's business climate of "just-in-time" deliveries, requires efficient and effective procedures to avoid losing sales or opportunities to bid. Better quality control can help speed decisions about what may be exported under License Exceptions, to whom, and under what conditions. Compliance administrators can develop procedures that allow for maximum flexibility as well as compliance.

Multinational companies have long ago learned the benefits of export compliance programs. Given the need to update those compliance programs to adapt to the ever-changing EAR, it is useful to set out the essential elements of a good compliance program.

12.2. Statement of Corporate Compliance Policy.

The first critical element of any compliance program is a clear demonstration of commitment by management. A solid statement of compliance policy should contain the following elements. A top management official of the company should sign the corporate compliance policy. The statement should make clear that it is the unequivocal policy of the company to comply with applicable export control laws. It is useful to specify the laws that will most often apply to the company (for example, the ITAR, the EAR, OFAC controls, and so on). Also, companies find it helpful to identify controls that might surprise company personnel, such as the fact that technology can be "exported" by transferring it within the United States to a foreign national (that is, a non-U.S.-citizen who does not hold a "Green card") and that the controls also apply to reexports of U.S. technology, U.S.-origin equipment, and foreign-made equipment containing U.S. components or that are direct products of U.S. technology. This is a good place to make everyone aware that U.S. export controls apply even to non-sensitive exports that someone in the

 bflowe@bcr-dc.com

company "knows" will be used in nuclear, missile, or chemical or biological weapons end-uses or by such end-users in certain countries. Export control officials prefer seeing a specific statement covering the nonproliferation controls that are currently the prime focus of U.S. export controls. Likewise, the statement might mention that no exports may be made to parties on certain lists who have broken U.S. export laws or who are designated as agents for certain embargoed countries. The policy statement should describe some of the penalties the company and its executives can incur for violating U.S. export control laws.

The statement should provide the names, positions, and phone numbers of company personnel in charge of implementing the compliance program to let employees know where to address questions. If the company chooses to place the statement of compliance policy in a stand-alone document, top management should distribute it to everyone in the company who has any involvement in exporting. This would usually include all sales, marketing, contracts, servicing, shipping, and other applicable employees. Procedures should ensure that it is provided to all new employees and to intra-company transferees. The company should have someone make sure that a fresh statement of compliance policy is disseminated on a regular basis, such as annually. Otherwise, staff tend to forget the policy. The export compliance administrator should ensure that this policy is reinforced by continuing training and education.

12.3. Key Personnel to Involve in the Program.

Management best demonstrates its commitment to an export compliance policy by allocating appropriate personnel and resources to support the compliance function. Who should perform what tasks differs from company to company. For instance, a company that sells and ships retail computer equipment on an immediate turnaround basis will have a much different compliance program organization than an aerospace company with low-volume, high-value sales. On the other hand, the spare parts and technical servicing areas of the aerospace company may require a compliance structure similar to that of the high-volume retail goods manufacturer. Each type of program must have dedicated personnel who are specifically assigned export compliance responsibilities if the program is to function efficiently.

Someone should have responsibility for each task in the compliance program, and the program should clearly describe the responsibility of each person or team. For instance, although functions can and should be allocated among different company personnel in a fashion most appropriate for a given company, a typical compliance program might assign responsibility in the following manner:

a. Oversight and Management Support. Designate someone in the upper management level, such as the president, general counsel, chief financial officer, or similar officer with responsibility for ultimate oversight of and support for the compliance program. This would include ensuring that adequate resources are provided and that those responsible for direct administration are performing adequately. Responsibilities might include the following:

i. oversee and support the compliance functions,
ii. maintain the regulations and other necessary resources,
iii. obtain and provide legal advice and interpretations as required,
iv. initiate audits and perform spot checks to ensure that the compliance program is functioning as intended,
v. police employment of foreign nationals to ensure that technical data exports to

 bflowe@bcr-dc.com

them (if any) are properly licensed,

vi. include appropriate clauses in international contracts to make sure they address appropriate export control provisions, and

vii. ensure that a new Statement of Company Export Compliance Policy is issued annually and that the compliance manual is updated regularly.

Upper management can oversee export compliance in a variety of ways. Whatever approach is chosen should actually function well in practice. One example worthy of consideration is the use of a Compliance Council chaired by a senior executive that reports to the Board of Directors. This mechanism was recently proposed in a report issued by a Hughes-commissioned task force that discusses export compliance "best practices".

b. Direct Responsibility for Export Compliance Administration. One person plus a backup, or members of a team as alternates, should have direct responsibility for administration of the compliance program. Job descriptions for this export compliance administrator function would include the following elements, some of which could be delegated to others:

i. Maintain a current set of the EAR, ITAR, OFAC regulations, and other appropriate regulations and related legal opinions and memoranda, articles, and other materials;

ii. Maintain all records required by the applicable export control regulations;

iii. Ensure that all sales and other personnel authorized to permit export shipments of products, software, and technical data are trained to spot "red flags" and review export compliance or, more realistically, are trained to refer to the export compliance administration for compliance screening all export shipments and domestic shipments that they have reason to believe may be exported;

iv. Monitor implementation of the compliance program, including (A) sending copies of the Manual and all other pertinent memoranda to affected personnel and to other appropriate persons; (B) making or supervising spot checks and periodic audits of records maintained pursuant to the export control laws and the company's compliance program; and (C) advising other personnel on questions about export control compliance;

v. Guard against export related transactions involving any parties on the "Denied Parties Lists" by reviewing updates to those lists against the company's customer lists, conducting an annual review of the company's customer lists against the Denied Parties Lists and end-use screening profiles, and ensuring that all export shipments (i) to new customers and (ii) involving in transit shipments are screened against the Denied Parties Lists;

vi. Keep informed about current developments concerning the applicable export control regulations and their implementation by subscribing to and reading the BIS's EAR and the updates in the Export Administration Bulletins, the ITAR, and other applicable regulations, and other updating services; consult with legal counsel and engineers, and attend seminars on new regulations and refresher courses, as appropriate;

vii. Ensure that company personnel involved in export control activities are adequately trained and maintain their knowledge and skills;

viii. Obtain legal advice whenever necessary to ensure compliance with the export control laws and regulations, report all alleged violations, disputes, and problems with export compliance administration or otherwise to the company official responsible for oversight and assist in their resolution as appropriate; and

ix. Implement procedures to ensure that a writing is obtained from foreign

 bflowe@bcr-dc.com

customers in cases in which the parties' intent is to shift export compliance responsibility to the foreign customer and prepare (or supervise the preparation of) a standard form that can be used for this purpose.

c. Export Compliance Team Members Doing Day to Day Processing. This could be the same person as the one responsible for administration in a small company or several different employees in a large company with multiple offices. Responsibilities for front-line work could include the following elements:

i. Review all export shipments and shipments to domestic customers where there is a reason to believe the product will be exported to (A) determine whether the shipment can be made under a General License, License Exception, or the designator "No License Required", or whether a new export license is needed, (B) if so, determine whether the shipment may be made under any existing license, and (C) apply for any new licenses that need to be obtained;

ii. Ensure that all international orders are placed on hold until export compliance/licensing reviews are completed and the shipment released under the proper license;

iii. Prepare and file all export license applications necessary, monitor the status of such applications, answer any inquiries on such applications as appropriate, and obtain approval of such licenses;

iv. Comply with all restrictions on the use of General Licenses, License Exceptions, or licenses, including conditions and provisos;

v. Communicate specific license conditions to the parties to whom the conditions apply and, when required by the license or when appropriate and feasible, obtain written acknowledgment of receipt of such conditions;

vi. Notify the compliance administrator whenever it appears necessary or desirable to prepare and obtain any BIS or DDTC bulk or comprehensive licenses for multiple shipments to distributors or other customers and work with the compliance administrator to prepare such applications to facilitate repeat shipments requiring licenses;

vii. Maintain records of export shipment documentation, including shipping invoices, export licenses, and any checklists and communications with the customers (in archives for at least five years beyond their expiration), shipping logs for License Exceptions LVS and TMP and other shipments that are limited or that must be tracked, filing timely license renewals and other amendments, as appropriate;

viii. Screen all export related transactions to guard against involving any parties on the current Denial Lists by reviewing all exports against the Denial Lists (to the extent not done by customer-based screening);

ix. Review all export related transactions against standards identifying risks of diversion, and conducting screening of all shipments to applicable countries to guard against shipments for unlawful end-uses or end-users (nuclear, missile, and chemical and biological weapons and military for CIV) and company participation in other illegal transactions or those presenting a high risk of diversion;

x. Maintain a copy of the Export Compliance Manual, current sets of the EAR, ITAR, and other relevant regulations and materials; and

xi. Keep informed about current developments concerning the EAR, ITAR, and OFAC embargo rules and other appropriate regulations.

d. International Shipping Supervisors. Specified shipping department employees and other appropriate individuals involved in exports should have export clearance functions

 bflowe@bcr-dc.com

similar to the following elements:

i. Ensure that no export shipment is made without an invoice, a waybill, and any required AES record properly completed to show (A) the applicable NLR, License Exception symbol, or license number, (B) the ECCN; (C) the value; and (D) the Destination Control Statement;

ii. Communicate with the export compliance team members to ensure that export shipments have been screened by them;

iii. Maintain a copy of Section 758 Export Clearance of the EAR and relevant shipping sections of the ITAR and ensuring that export shipments comply with the requirements of those Sections, including lodging State Department Licenses with Customs and maintaining decrementing logs against shipments to ensure that authorized volumes and values are not exceeded;

iv. Maintain a copy of the Product Matrix, export clearance checklists, and other documents to assist in export screening;

v. Have clear authority to detain any shipment as necessary until they receive approval from the export compliance administrator that the shipment is in compliance with the export control laws and may be released for export; and

vi. Maintain copies of all export shipping records for at least five years.

Many companies engaged in sensitive military or nuclear activities also police e-mail and fax capabilities in connection with security clearance procedures to control, or at least provide clear warnings against, unauthorized transfers of technical data without a license. Some companies include appropriate warnings in international travel documents to remind personnel of the applicability of the export control laws and need for compliance with goods and technology transfers.

e. <u>An Export Classification Engineer</u>. It is often helpful to assign someone with technical knowledge of the company's products and technology to assist the export compliance administrator in reviewing all new products and improvements to determine whether their specifications qualify for NLR or License Exceptions GBS, CTP, TSU, or CIV shipment, and whenever the export compliance administrator otherwise may need appropriate technical information for export licensing activities. This engineer should assist the export compliance administrator to maintain the Product Matrix, which presents the results of these classifications, and copies of all information obtained from suppliers and government agencies (DDTC, BIS, and so on) that are used to develop and maintain the Product Matrix.

It is important to build redundancy into key positions so that the company can fulfill time-sensitive compliance functions whenever a key person is absent.

12.4. <u>Order Processing Controls</u>.

This section addresses the screening elements of export compliance programs framed around order processing because the company's means of processing orders will tell someone where these screening can best be performed and by whom. In this context, the term "orders" can mean purchase orders, back orders, requests for quotes or proposals, invitations to bid, marketing projects, and similar means that stimulate a company to make an export. Once one determines how all export shipments are made and by whom, the company can determine how best to structure the essential elements of its export compliance program to ensure that it implements requisite compliance functions at the earliest and also the last possible stage.

 bflowe@bcr-dc.com

Effective compliance procedures should dovetail with the procedures by which a particular company already does business. This model addresses the essential compliance elements for most companies, though some elements may not be necessary for a given company. Attached is a form of Customer Export Compliance Checklist Reference Form that can be used to document compliance screening described below. Procedures must be developed to support it.

12.4.1. Product and Country Screening. Generally, companies find they can accomplish export compliance functions most efficiently if they develop and maintain a particular tool – a matrix of their products showing applicable export controls by country ("Product Matrix"). With a well-developed Product Matrix, export compliance staff can generally tell at a glance:

(a) the applicable ECCN for those covered by the EAR, the Munitions List Category, or other appropriate classifications that show the agency having jurisdiction over the export,

(b) whether a given product may be exported to a given country under a License Exception, or whether a License is required, and if so, from which licensing agency (Commerce, State, OFAC, or others), and

(c) in many cases, whether a license already covers the shipment or, if a new one needs to be obtained, under what conditions, and in what length of time.

In *Iran Air v. Kugelman*, 996 F.2d 1253 (D.C.Cir. 1993), Justice Ginsburg, then writing for the D.C. Circuit Court of Appeals, held that an export of a product without a license when one is required because of the export classification is a strict liability offense. This means that one violates the law if one exports a licensable item under a general license as a result of a mistaken classification. Accordingly, a Product Matrix is essential for high volume shipments. Companies can rarely afford the time, expense, and manpower of having top-level company engineers examine and classify each and every product and the export compliance administrator make licensing decisions on an order by order basis.

Appropriate matrices can be detailed and complex, such as those providing ECCNs and available Licenses, License Exceptions, or Exemptions for applicable country groups for each product number. Some may even prefer to use and apply the detailed country matrix in Supp. 1 to Part 738 of the New EAR. A Product Matrix can be more simple, showing groupings of products by ECCNs, or Munitions List designations, and available License Exceptions by applicable country groups. This simpler model should provide a clear indication of the points at which products will fall into other ECCNs, including categories for future products that may be subject to more stringent controls. It should also show which products will require reporting so that the administrators can establish a system to gather data accurately and on a timely basis for required reports to BIS.

The exporting company need not reinvent classifications of products that it does not manufacture. The suppliers of key products increasingly can usually be persuaded to provide applicable classifications for their products to resellers or manufacturers using them.

Instructions should clearly inform export compliance personnel that no product, technology, or software that is not listed on the Product Matrix may be released for export without

 bflowe@bcr-dc.com

authorization from designated compliance personnel. Procedures should ensure that the export administrator is informed of new products to be introduced in order to add them to the Product Matrix so they can be authorized for export in a timely fashion.

12.4.2. Licensing Determinations. Export compliance staff should use the Product Matrix and other screening procedures to determine whether a License Exception is available or whether a License is needed. They should also be instructed on the restrictions applicable to use of License Exceptions and Licenses. If any product is shown on the Product Matrix as not being eligible for shipment without a License, they should determine whether it may be shipped under an existing License, including a bulk type of license. If not, they should place a hold on the order and initiate appropriate procedures to obtain the License from the appropriate agency. They should inform appropriate staff of the expected time needed to obtain the applicable license.

The company should design some method to ensure that the appropriate screening has been performed and to communicate the required export clearance information to appropriate personnel for completion of shipping paperwork. Many companies find it useful to prepare a short "Export Compliance Checklist" form with blocks to be checked and signed by export compliance staff member. Although compliance staff may balk at the idea of completing such forms initially, they soon find it simple, especially if it is done online and via customer based screening (so that transactions simply make sure the screening were performed). These checklists are invaluable to give auditors and export enforcement officials a sense of confidence that the company has performed appropriate export compliance reviews. The fields to be completed also serve as helpful reminders. Export compliance screening procedures become rote over time and steps may easily be omitted if left to memory.

12.4.3. Denied Parties Lists Screening. It is essential to develop a screening mechanism to prevent shipments to entities on the many lists published by various government export control agencies of parties with whom it is illegal to deal in export transactions (at least without a license). Parties on the various Denial Lists maintained by BIS, OFAC, and DDTC, among others, generally have either violated U.S. export control laws or have been designated as agents of embargoed countries. The essential requirement of a screening procedure is to identify and prevent shipments to parties on these denial lists until someone in the company can determine whether the shipment might be permitted and under what circumstances. Violation of the Denial Orders is generally considered a strict liability offense given that persons are charged with constructive knowledge of anything published in the *Federal Register*, whether they in fact know it or not.

The first essential element of denied parties screening is to obtain all the applicable lists. This is easier now because U.S. export control agencies have finally cooperated and BIS is now publishing a consolidated list, including the BIS Denied Persons List, OFAC lists of Specially Designated Nationals ("SDNs") for embargoed countries or other reasons (*e.g.*, terrorism), State Department lists of (i) debarred parties and (ii) entities subject to missile technology, nuclear, or chemical and biological weapons sanctions, entities which BIS has informed exporters require a license for proliferation reasons ("Entity List"), and Unverified List of Suspect Foreign End-Users (it is a red flag if party on latter list is involved). The consolidated list is available at www.Export.gov. Several third-party services also provide current consolidated Denied Parties Lists (some even include lists of parties targeted by the EU, United Kingdom, Japan, and other countries) in computerized form, including online databases with search procedures. A procedure for automated screening of these consolidated lists works most efficiently for most

high volume exporters.

Whatever method a company chooses for obtaining the relevant Denial Lists, the Export Compliance Procedures Manual should include procedures for making someone responsible for obtaining the Denial Lists and updates thereto and for disseminating them to appropriate personnel within the company as well as to other sites, foreign consignees, and to other distributors that the company desires to ensure maintain appropriate export compliance programs. The method of distribution should include some form of acknowledgment of receipt from the other companies and verification of receipt in-house. Timeliness of distribution is a practical issue that exporters faced. Legally, companies are liable for doing business with Denied Parties from the moment they are published in the *Federal Register*. Some agencies, such as OFAC and State, even include effective dates that predate such publication, but it is virtually inconceivable that enforcement officials would bring an action against a company that traded with a Denied Party absent actual knowledge of that status before publication provides constructive notice. The only way to stay current is by monitoring the *Federal Register* and updating computerized Denial Lists on a daily basis or by subscribing to online services, although these are usually somewhat behind. Because few companies have ever found more than a handful (if that many) of customers on the Denial Lists after screening thousands of shipments, companies that use manual lists often decide that periodic distribution of updates is sufficient. They knowingly take what they determine is a relatively minor business risk that is outweighed in their case by the expense of maintaining a perfectly up-to-date list. There are no reported cases of enforcement actions taken against companies that did business with Denied Parties within a few weeks after publication, although no one wants to be the first. Each company must decide what method of subscribing to and updating the Denial Lists is most appropriate to its level of business. Now that BIS is publishing a consolidated list, it should be easier.

12.4.4. Customer or Transaction Based Screening. Depending on the nature of its sales, a company may find it most efficient to screen Denial Lists against customer lists, on a transaction by transaction basis, or some combination thereof. Companies shipping mostly to repeat customers will generally find it more efficient to screen their customer lists against the Denial Lists and updates thereto. Companies shipping to few repeat customers may find that screening each transaction against the current Denial Lists is more efficient. Whatever method or combination of methods is used, the company should make sure to close any gaps in the screening. Generally, the export compliance staff should screen known principals of the customer against the Denial Lists as well as the customer because denied parties often start doing business again under another name.

a. Customer-Based Screening Techniques. Customer-based screening techniques should provide a method to ensure review of updates to the Denial Lists against the customer lists. The person responsible for the review should also review the entire customer list against the Denial Lists on an annual basis. The compliance procedures should require them to document each of these reviews (for instance, by initials of the reviewer and date on the cover page of the applicable Denial List update or annual review list). Companies with procedures that do not allow any shipment to be made to a new customer without a customer number request the new customers to be screened by the party responsible for assigning said number, for instance the accounting department which is also reviewing credit or other aspects of the customer. Some method of ensuring that all new customers are screened is necessary for customer-based screening to be effective.

 bflowe@bcr-dc.com

b. Transaction-Based Screening. Transaction-based screening is fairly straightforward. To ensure that the company does not participate in any export related transaction with a party on the Denial Lists, the export compliance staff must review each new export order (however defined) for each and every customer against the current Denial Lists prior to shipping the order. If there is a significant time lag between the initial review and shipment, the company may wish to have a secondary screening prior to shipment to ensure that the party has not been added to the Denial Lists. The procedures should provide a method for documenting such review (such as with the export compliance checklist, discussed above.) The reviewers must maintain current copies of the Denial Lists to accomplish their screening. Automated screening is perhaps the best method of accomplishing this task given the likelihood that human reviewers will sleep through the one customer on the Denial List out of thousands reviewed, although there are yet no satisfactory computer programs.

12.4.5. Authorization to Hold Shipments. Export compliance personnel must have explicit authorization to hold export shipments whenever anyone is found to be listed on a Denial List. The hold-shipment order should apply to all orders for that customer. All appropriate persons at the company, including particularly all shipping department personnel, must be notified in writing not to ship anything to said customer until instructed by the responsible person that shipments may be resumed. The export compliance administrator should investigate the matter with the applicable export control agency. Often, hits on Denial Lists screening result from similar names. If the agency confirms that the party is one still subject to denial, the hold-shipment order should remain standing. If the agency confirms that the party is not the same, the export compliance administrator should document this fact and authorize the shipment's release.

12.4.6. Diversion Risk Screening. Export compliance staff should review each export customer (and each domestic customer that they have reason to know will export the products) to assess the risk that the customer might divert the shipment to destinations that are not authorized under the export control laws. The export compliance administrator should ensure that the parties doing any customer based screening (such as accounting) as well as the export compliance staff review both the customer and the transaction as well as any intermediate consignees against appropriate "red flag indicators" such as those attached hereto. This is not as onerous a requirement in practice as it might seem. The "red flag indicators" are illustrative of many types of factors that can arise to make a given customer or transaction seem like something is not quite right. Companies have applied such "red flag indicators" for years under more common name, "passing the smell test".

12.4.7. Apply "Know Your Customer Guidance" in Conducting Screening. Administrators should follow the BIS "Know Your Customer Guidance" attached hereto to help determine when export control officials expect them to inquire further in a transaction and when they should apply for a license or end-user check even for shipments that otherwise qualify for a License Exception. If the customer shows any of the types of suspicious characteristics set forth in applicable "red flag indicators", the export compliance staff should initiate follow-up inquiries to determine if there are legitimate explanations. In any case where they are not satisfied with the explanations, they should place the order on hold and shall refer the matter to the export compliance administrator, in-house counsel, or other appropriate persons for further investigation and decision. The latter, if not satisfied after further appropriate investigation, should consider contacting BIS or other appropriate export control agencies directly to explain the reasons for the concern and to determine if there is information available on the customer's reliability.

 bflowe@bcr-dc.com

In any case where concerns are not resolved satisfactorily, the company should either (a) cancel the order, or (b) apply for a License with full disclosure of the facts that gave rise to the concern.

BIS helpfully narrowed the application of excessively broad end-use and end-user controls to those activities and exports that "directly" support applicable missile or chemical and biological weapons activities in a *Federal Register* interpretation published in December 1993. (That interpretation has never made it into the EAR, but we have an advisory opinion confirming it is still the policy.) Also, BIS can foist knowledge on exporters by informing them, directly by letter or constructively through amendments to the EAR published in the *Federal Register* or elsewhere that are available to all exporters, that a license is required for certain activities or exports due to an unacceptable risk of use in or diversion in troublesome missile activities.

12.4.8. Sensitive Nuclear End-Users and End-Uses Screening. Regardless of whether commodities or software otherwise qualify for export under NLR or License Exceptions to a given destination, a company must obtain a license when a company "knows or has reason to know" that said product will be used, directly or indirectly, in a country that is not listed in Supplement 3 to EAR Part 744 or Canada in any of the "sensitive" nuclear applications described below, regardless of whether it is specifically designed or modified for such activities. Likewise, no one may make exports of any technology other than public domain information (or "operation technical data" or "sales technical data" under TSU only to countries listed in Supplement 3 and Canada) where the exporter knows or has reason to know that said technology will be used, directly or indirectly, in a in any of the "sensitive" nuclear applications described below. Accordingly, exporters should establish some method of screening to ensure that they do not make such knowing exports without first doing some due diligence and generally applying for and obtaining a License. (EAR § 744.2.)

These restrictions apply to the following activities:

a. Nuclear explosive activities, including research on or development, design, manufacture, construction, testing, or maintenance of any nuclear explosive device, or components or subsystems of such a device;

b. Unsafeguarded nuclear activities including research on or development, design, manufacture, construction, operation, or maintenance of any nuclear reactor, critical facility, facility for the fabrication of nuclear fuel, facility for the conversion of nuclear material from one chemical form to another, or separate storage installation where there is no obligation to accept International Atomic Energy Agency (IAEA) safeguards at the relevant facility of installation when it contains any source or special fissionable material (regardless of whether or not it contains such material at the time of export), or where any such obligation is not met;

c. Safeguarded and unsafeguarded nuclear fuel cycle activities, including research on or development, design, manufacture, construction, operation, or maintenance of any facilities or components of facilities for (i) chemical processing of irradiated special nuclear or source material, (ii) heavy water production, (iii) separation of isotopes of source and special nuclear material, or (iv) fabrication of nuclear reactor fuel containing plutonium.

 bflowe@bcr-dc.com

(EAR § 744.2.) The most sensitive countries are listed in Country Group D:2 (Supp. 1 to EAR Part 740).

12.4.9. Missile Technology End-Uses and End-Users. Regardless of whether a product otherwise qualifies for export under NLR or License Exceptions to a given destination, a company must obtain a license from BIS when it "knows" that any product, technology, or software is to be used in the design, development, production, or use of rocket systems, missiles, or unmanned air vehicles anywhere in the world. (EAR 744.3.) Several items, software, and technical data require licenses by their nature because they are controlled for missile technology reasons, regardless of whether the products, software, or technology are specifically designed for use in missile activities. Technical data that is in the public domain such as books, films, etc. are the only items excluded from these prohibitions.

In the missile technology and chemical and biological weapons areas, the above prohibitions also apply to exports and reexports by "U.S. persons" regardless of whether the items themselves are subject to U.S. jurisdiction. No U.S. person may perform any contract, service, or employment that they know will assist in the design, development, production, or use of missiles in or by a Supplement 1 country unless they first obtain a license. And, no U.S. person may knowingly support in any other way any such activities, including financing, transportation, freight forwarding, or other facilitation regardless of whether that person is the actual exporter or reexporter.

Many companies simply add Supplement 1 entities to the Denial Lists to facilitate screening of shipments for those entities. Missile technology prohibitions apply to exports to any other entity in Supplement 1 countries that the exporter knows is involved in missile related activities.

Pursuant to certain provisions of the National Defense Authorization Act for Fiscal Year 1991 (50 U.S.C. app. § 2410b), sanctions may be imposed against persons that engage in the proliferation of missile technology. Sanctions may include, in the case of U.S. persons, the denial of export licenses for all items controlled by the EAA for a period of two years as well as other penalties under the EAA. In the case of foreign persons, sanctions may include the denial of export licenses for the transfer of items controlled by the EAA to the sanctioned person or the prohibition, for a period of not less than 2 years, of the importation into the United States of products produced by the sanctioned party. There are several exceptions to the prohibition against importation by a sanctioned party.

The application of these sanctions to entities involved in the nuclear and missile programs in India, Pakistan, China, and Russia caused great competitive problems for exporters wishing to do routine business with those entities. A significant interpretation of these restrictions came when BIS published guidance in December 1993 limiting the application of the scope of the "know or is informed" language of the Enhanced Proliferation Control Initiative ("EPCI") missile, chemical and biological weapons license requirements to knowing or being informed that the goods will be "directly employed" in the design, development, production or stock piling of such weapons. The catch-all rule had been broadly interpreted by BIS to require a license for anything, no matter how benign and regardless of whether it directly contributed to an offensive nonproliferation activity if it was being exported to an end-user who was engaged in such activities. This December 1993 interpretation allowed BIS to return a large backlog of such cases as not needing a license. It gives the exporter more discretion to determine that particular

exports do not require such a license because they will not be "directly employed" in the offensive activities, to his/her knowledge. It is still valid even though it was not published in the EAR.

12.4.10. Chemical and Biological Weapons End-Uses and End-Users. Regardless of whether a product otherwise qualifies for export under NLR or a License Exception to a given destination, a company must obtain a license when it "knows" that said product will be used directly in the design, development, production, stockpiling or use of chemical or biological weapons ("CBW") in or by any country. (In March 2005, BIS amended the EAR by expanding the country scope from D:3 to all destinations of the chemical and biological weapons end-user/end-use controls in Section 744.4(a) to conform with the country scope of the "catch-all" provisions in the Australia Group ("AG") "Guidelines for Transfers of Sensitive Chemical or Biological Items." Although some products are controlled because they are designed to be used directly in such activities, this prohibition on exports under NLR and License Exceptions applies to all products that the company knows will be used directly in chemical or biological weapons activities any country. (EAR § 744.4, as amended by 70 *Fed. Reg.* 16110 (Mar. 30, 2005).) As with missile activities, technical data in the public domain (books, films, and so on) are the only items excluded from these prohibitions.

These prohibitions apply to exports and reexports by "U.S. persons" regardless of whether the items themselves are subject to U.S. jurisdiction. Also, no U.S. person may perform any contract, service, or employment that they know will assist in the design, development, production, stockpiling, or use of CBWs in or by a Group D:3 country unless they first obtain a license. No U.S. person may without a license or other authorization from BIS participate in the design, construction, export, or reexport of a whole plant to make chemical weapons precursors identified in ECCN 1C350 except on Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom. Finally, no U.S. person may knowingly support in any other way any such activities, including financing, transportation, freight forwarding, or other facilitation regardless of whether that person is the actual exporter or reexporter. (EAR § 744.4.)

Pursuant to the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (50 U.S.C. app. § 2410c), sanctions may be imposed against foreign entities that knowingly and materially contributed to the efforts by any foreign country, project, or entity to use, develop, produce, stockpile, or otherwise acquire chemical or biological weapons. Sanctions against the foreign entity, including the foreign parent, subsidiary, or affiliate of the foreign entity if such parent, subsidiary, or affiliate knowingly assisted in the activities that were the basis of the sanctions, include a bar on U.S. procurement of, any goods or service from the sanctioned entity(ies) and prohibition on importation into the United States of any products produced by the sanctioned entity(ies). These sanctions have not yet had the same impact as the missile sanctions.

As in the case of missile technology, BIS helpfully narrowed the application of these excessively broad controls to those activities and exports that "directly" support applicable CBW activities. Also, BIS can foist knowledge on exporters by informing them, directly or constructively amendments to the EAR published in the *Federal Register* or elsewhere that are

available to all exporters, that a license is required for certain activities or exports due to an unacceptable risk of use in or diversion in CBW activities.

12.4.11. Military End-Uses and End-Users for CIV, CTP, Iraq, and China Exports. One may only make exports under License Exception CIV or CTP to D:1 countries if the shipments are both (a) to civil end-users and (b) for civil end-uses. If the export is either to a military end-user (whether or not for civil use by that end-user, such as in the PX) or to a civil end-user for "known" military end-use (such as to a government contractor for use in a military contract), a shipment under CIV will be illegal. Exporters shipping under CIV will thus need to screen their shipments to ensure against shipping (a) to military end-users and (b) for known military end-uses. Likewise, exporters shipping certain 3A991 microprocessors must similarly screen.

A military end-use and end-user control was imposed in 2004 on exports and reexports to and transfers within Iraq. In June 2007, BIS imposed a new end-use control on exports and reexports to and transfers within China of certain items for military end-use.

12.5. Screening Imports of Arms, Destructive Devices, and Nuclear Materials.

U.S. exporters who import items on the Munitions Import List must also establish procedures to ensure against imports of such items that do not comply with Bureau of Alcohol, Tobacco, Firearms and Explosives of the Justice Department ("BATF") and/or DDTC registration, licensing, permitting, and tax requirements. These requirements do not apply to technology or encryption imports or to any other export control agency's items other than nuclear materials. As this does not apply to most companies, further discussion is deferred.

12.6. Special Guidance for Controlling Exports of Technology and Software.

Technical data and software exports should be subjected to the same procedures described above. Because the law and government policies concerning technical data and software are complex, this discussion summarizes in more detail the current rules and special procedures for handling exports of technical data and software. Company export compliance administrators should be consulted before any technical data or software that is not in the public domain or listed on the Product Matrix is exported.

12.6.1. Technical Data. In general, five basic rules govern.

a. First, technology and software generally available to the public at no charge or a charge that does not exceed the cost of reproduction and distribution may be exported to all countries without the need for a License or a License Exception because it is outside the scope of the EAR. (EAR § 734.3(b)(3).) Although no symbol is required for export documentation, exporters may use the symbol "TSPA" on shipping documentation to cover such exports. EAR 758.1(g)(3). Most technology data that is exported qualifies for export under TSPA. (For instance, most if not all manuals and software manuals are available free of charge to anyone (or at nominal charges to cover only the reproduction costs). Accordingly, the information in these manuals may be exported under TSPA.)

See EAR § 734.3(b)(3) and other sections referenced there for details on what is considered publicly available. Technology is publicly available when it is (A) "published" and

 bflowe@bcr-dc.com

becomes generally accessible to the interested public in any form, including publication in any media available for general distribution to persons interested in the subject matter, either free or at a price that does not exceed the cost of reproduction and distribution, readily available at libraries open to the public or at university libraries, in patents and published patent applications available at any patent office, release at an open gathering; (B) fully disclosed in a patent application on file with the U.S. Patent and Trademark Office for which the applicant has received authorization for foreign filing or applications filed in a non-U.S. country; or (c) fundamental research, as defined in EAR § 734.8. Full exploration of these terms is beyond the scope of this paper. Exporters are advised to document the classification in close cases or at least establish clearly defined methods for their analysis. Some exporters of sensitive technology publish it on the web to ensure that it is in the public domain. Others will donate manuals and other materials to the library at an engineering school to ensure there is no doubt. Note that just because one publishes an article on technology does not mean that proprietary applications of that technology are also in the public domain. A U.S. person has the First Amendment right to put technology in the public domain, but exporters should be careful about treating versions as public domain that they also in other contexts treat as subject to confidentiality agreements. The facts in the application of the public availability exemption are often nettlesome.

The various OFAC sanctions regulations apply similar exemptions for "informational materials" found in the so-called Berman Amendments to the Trading with the Enemy Act and the International Emergency Economic Powers Act. Thus, qualifying public domain technology is exempt from export controls even to embargoed countries.

b. Second, "sales technical data" supporting a prospective or actual quotation, bid, or offer to sell, lease, or otherwise supply a controlled item may be exported under or License Exception TSU to any country (except possibly Iran), *provided* that the data is of the type customarily transmitted with such bids, and the export will not disclose detailed design, production, manufacture, or reconstruction of the quoted item or its product. (EAR § 740.13(b).)

c. Third, "operations technical data" that is the minimum necessary for the installation, operation, maintenance (checking), and repair of products exported under NLR, License Exceptions, or Licenses may be exported under License Exception TSU to any country to which the equipment was legally exported (except possibly Iran). (EAR § 740.13(a).) This does not allow release under License Exception TSU of the repair "technology" controlled by 1E002.e, 1E002.f, 8E002.a, or 8E002.b. (EAR Part 774, Supplement 2, General Technology Note. This restriction, if meaningful, should be incorporated into EAR § 740.13(a).) To the extent that manuals are not publicly available as described above, they are often exportable under License Exception TSU as "operations technical data" to customers who have received or are receiving applicable products.

d. Fourth, to the extent that TSPA or TSU are not available, all technology to be exported must be classified under the applicable ECCN in the Commerce Control List ("CCL") set forth in Supplement 1 to EAR 774. That classification (in part E of each CCL category) will provide guidance on whether NLR (as a result either of not having an ECCN and thus designated EAR99 or applying the applicable ECCN and the Country Matrix) or License Exceptions TSR or TSU may be used for the export to a particular destination.

i. If no ECCN is applicable (EAR99) or the application of the data's ECCN to the Country Matrix in Supplement 1 to EAR 738 shows NLR, the data may be

exported under NLR to all appropriate destinations except the embargoed destinations;

ii. If the applicable ECCN states "TSR: Yes" then it may be exported under License Exception TSR *only* to destinations in Country Group B (Supp. 1 to EAR 740), subject to any other specific destination restrictions of that ECCN. (EAR § 740.6.) In order to use License Exception TSR for such an export, the exporter must first obtain a written assurance from the customer that neither the technical data nor the direct product thereof will be reexported to unauthorized destinations without Commerce Department authorization. (Several versions of such written assurance provisions can comply with the requirements of EAR § 740.6(a)(3).)

Classifying technology in a practical setting can be almost as difficult as classifying and capturing particles of smoke. Some companies have developed for their research and development engineers who must share technology with foreign nationals and other offices around the world certain "Technology Matrices" setting out those technologies that require a license for different layers of countries (*e.g.*, those to which they can otherwise export technologies under License Exception TSR assuming they have a written assurance on file, etc.). Such lists and other tools, with training, can help alert engineers when licenses might be needed for certain technologies.

Pay close attention to the structure of the technology controls in the CCL and the important definitions of "development", "production", and "use". Some technologies are controlled under particular ECCNs only for some, but not all three purposes, whereas the broadest controls in certain ECCNs apply to all three. *See* L. Christensen, "Technology and Software Controls under the Export Administration Regulations," Coping with U.S. Export Controls 2001 663-67 (PLI 2001).

The classification question can be confusing due to one of the provisions of the General Technology Note that states: "'Technology' 'required' for the 'development', 'production,' or 'use' of a controlled product remains controlled even when applicable to a product controlled at a lower level." (EAR § 774, Supp. No. 2.)

EAR Part 772 defines the term "required" narrowly as it applies to technology:

> "Required". (General Technology Note) (Cat 4, 5, 6, and 9) – As applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different products. For example, assume product "X" is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies "A", "B", and "C" allow production at no more than 399 MHz, then technologies "A", "B", and "C" are not "required" to produce the controlled product "X". If technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can produce product "X" that operates at or above 400 MHz. In this example, technologies "D" and "E" are "required" to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

 bflowe@bcr-dc.com

Under these provisions, for a technology to be controlled under 4E001 it must be "peculiarly responsible" for enabling the 4A or 4D item in question to achieve the performance parameter required for control. If the controlled item in question is a "digital computer" under 4A003.b, the technology must be "peculiarly responsible" for enabling the "digital computer" to exceed 0.75 weighted TeraFLOPS (or other applicable control parameters).

A deep level analysis is required to determine just what are the specific technologies involved that are "peculiarly responsible" for producing end products that achieve technical specifications that exceed the ECCN 4A003 control parameters. One should classify those technologies and determine if they are, in fact, used to produce a decontrolled product. The peculiarly responsible technologies may in fact all be Category 3 technologies rather than Category 4. We have long posited, with many BIS officials in agreement, that the only technologies "required" to develop what at that time were export controlled personal computers were the technologies to produce microprocessors, and that said technologies are controlled by Category 3, not Category 4. This is a factual question that must be applied by each company. The distinction can be important when applying controls on technology exports to Group B countries because there is no CTP limit for ECCN 3E001, but there is a limit of 0.5 weighted TeraFLOPS for TSR exports controlled by ECCN 4E001.

e. Fifth, to the extent that NLR or a License Exception is not available to export particular technical data, the company must apply for and obtain a License before making physical export or disclosing the technology to a foreign national. *See* EAR § 748.8(o) and Supplement 2(o) for unique requirements for technology license applications.

Important: Disclosure of "technical data" by any means in any place, including visual observation or oral disclosure in the United States to foreign visitors, constitutes an "export" within the meaning of the Regulations. (EAR § 734.2(b).) For export control purposes, the term "foreign national" means any person who is not a U.S. citizen or permanent resident (*i.e.*, holds a "Green Card"), or in the case of reexports, is not a permanent resident under the laws of the location of "deemed reexport".

12.6.2. Software. Export administrators should use the following line of analysis to determine the proper licensing requirements for particular software products to specific destinations. Points E through I apply to most software programs, and most software currently exported qualifies for export under NLR or License Exception TSU to all destinations except for Country Group E:1 (Cuba, Iran, North Korea, Sudan, and Syria).

A. All software programs designed for military uses require export licenses to all destinations from the State Department's Directorate of Defense Trade Controls under the ITAR. Other provisions in this analysis will not apply to such software. Commercial software that contain certain encryption functions (with a few exceptions for authentication, access control, and decryption-only proprietary software protection routines) were covered by the ITAR until December 30, 1996; they are now covered by the EAR, but are often subject to stringent licensing requirements.

B. Software that is publicly available at no charge other than nominal copying charges (no license fees), such as in a library or on a public electronic bulletin board, may be exported to any destination without a license (using TSPA, as described above for technical data). Note that encryption software is not eligible for this exclusion.

 bflowe@bcr-dc.com

C. All software programs not eligible for TSPA or TSU exports that are exported to Country Group E:1 countries require a License either from BIS or under the sanctions regulations administered by the Office of Foreign Assets Control of the Treasury Department for those destinations.

D. Software programs exported to Canada do not require either NLR, a License Exception, or a License except for the few types of software classified under an ECCN which states specifically that a License is required for Canada. License requirements for Canada presently are limited to software related to nuclear activities.

E. Most software subject to the EAR is classified under an ECCN in the Commerce Control List ("CCL") in Supplement 1 to EAR Part 774. If not specifically listed in an ECCN, commercial products are eligible for export under NLR using the designation EAR99 (instead of an ECCN) to all countries other than Cuba, Iran, North Korea, Sudan, and Syria. (*See* I. below.)

F. Mass-Market Software. Software, regardless of classification under the CCL, may be exported to all destinations except for Cuba, Iran, North Korea, Sudan, and Syria under License Exception TSU if it is generally available to the public by being:

i. Sold from stock at retail selling points (without being sold only bundled with hardware) by means of:
   (a) Over the counter transactions;
   (b) Mail order transactions; or
   (c) Telephone call transactions; and

ii. Designed for installation by the user without further substantial support by the supplier (telephone help lines are not a problem).

EAR § 740.8(d) and the General Software Note in Supplement 2 to EAR Part 774. Mass-market software qualifies for TSU export as described above regardless of what its classification under the CCL otherwise would be. No software with encryption functions should be exported as mass-market software without clearance by the export compliance administrator by designation on the Product Matrix or otherwise in writing.

G. Operation software that is the minimum necessary to operate equipment authorized for export under License, License Exception, or NLR may be exported in object code only under License Exception TSU to all destinations to which the applicable equipment was lawfully exported. (EAR § 740.8(a).) To the extent that any operating software programs do not qualify as mass-market software, the export compliance administrator should seek clarification of how the term "minimum necessary" should be applied.

H. Exports of software updates or releases designed solely to fix "bugs" may be made under License Exception TSU to any destination to which the software for which they are required was legally exported or reexported, provided that such updates are provided to the same consignee and do not enhance the specified functional capabilities of the initially exported software package. (EAR § 740.8(c).)

I. All software that is subject to the EAR is covered by a specific ECCN in the CCL or is eligible for the designator EAR99 and thus export to all but Cuba, Iran, North Korea,

Sudan, and Syria under the designator NLR. If none of the above described License Exceptions is applicable, the exporter must work with engineers to classify the software under the applicable ECCN and apply the Country Matrix in EAR Part 738 to determine if NLR or a License Exception applies or if a License is required for a particular destination.

(i) Classify the software. Software is specifically covered under sub-category D of each of the following CCL categories:

0. Nuclear Materials, Facilities, Equipment, and Miscellaneous
1. Materials
2. Material Processing
3. Electronics
4. Computers
5. Telecommunications and Information Security
6. Lasers and Sensors
7. Navigation and Avionics
8. Marine
9. Propulsion Systems, Space Vehicles and Related Equipment

Most general purpose computer software is classified under ECCNs in Category 4D or EAR99 if not covered by a specific ECCN thereunder. Most telecommunications software is classified under ECCNs in Category 5D or EAR99 if not covered by a specific ECCN. However, certain specialty software is covered by other categories.

(ii) If EAR99 applies or the applicable ECCN "Requirements" section combined with the Country Matrix in EAR Part 738, Supplement 1 do not result in an X in the box for License Requirements to the applicable destinations, it may be exported under NLR to all destinations other than Cuba, Iran, North Korea, Sudan, and Syria, any others specified in the applicable ECCN or the Country Matrix. (This assumes that other screens (*e.g.*, Denial Lists, end-user, and end-use) are cleared.)

(iii) If an applicable ECCN states "TSR: Yes", then it may be exported under License Exception TSR to destinations in Country Group B (Supp. 1 to EAR 740). In order to use License Exception TSR for such an export, the exporter must first obtain a letter of assurance from the customer that the software will not be reexported to unauthorized destinations without Commerce Department authorization.

(iv) License Exceptions TSU, ENC, and KMI may apply to certain encryption software classified under ECCN 5D002 after one time review by BIS. Other License Exceptions apply to certain exports under limited circumstances (*e.g.*, GOV, TMP, BAG, LVS, RPL, APR).

(v) If NLR or License Exceptions are not available, the company must apply to BIS for a *License* in accordance with the requirements of EAR Part 748 to cover the export.

If in doubt as to the proper classification, one may apply to the Commerce Department for clarification of the classification pursuant to the provisions of EAR Part 748.3.

 bflowe@bcr-dc.com

J. All *media* by which software is conveyed have been decontrolled.

12.6.3. Reporting Requirements. Part 743 of the EAR requires reports for exports under certain license exceptions, including License Exception TSR. Exporters should take special care to ensure that they meet these requirements in a timely and accurate fashion, especially since it is the Office of Export Enforcement that reviews reports. BIS has provided some special guidance to minimize reporting under License Exception TSR given that technical data exports are often repetitive. First, one does not need to report "deemed exports" to foreign nationals in the United States. Second, exporters need only report only first transfer to foreign entities or U.S. subsidiaries under License Exception TSR, and to list the quantity as "1" for each TSR transfer. Finally, one need only report future TSR transfers to same end-user only if scope of controlled technology changes. No reports of reexports under License Exceptions or NLR are required.

12.6.4. Suggested Procedures. A company's export compliance administrator should review and classify all software programs and technical data (such as user manuals) normally exported and describe on the Product Matrix the extent to which NLR or License Exceptions are available for their export. Employees should not authorize the export of any technical data or software unless they have made an export license determination pursuant to its description on the Product Matrix or have consulted with and been advised by the export compliance administrator as to the appropriate export license that may be used. When applying for Licenses for equipment, list the applicable software on the license application regardless of whether it may be exported under a NLR or License Exception.

The compliance program should require the Human Resources Department to alert the export compliance administrator whenever the company employs a foreign national who is not a permanent resident so that appropriate decisions can be made on whether disclosure of non-public technical data or source code to that national can be made under NLR or License Exceptions or require Licenses. The export compliance administrator should work with the applicable supervisor to ensure that such employees are restricted from access to technical data until the proper export license has been applied in a manner consistent with employment laws. (Most such foreign nationals will be eligible to receive most technical data of the type used by most companies under NLR or License Exception TSR provided that they sign an appropriate written assurance against reexport of such data or its direct product.)

12.7. Export Clearance – Shipping and Receiving as Ultimate Control Point.

A company is responsible for the proper use of NLR, License Exceptions, and Licenses and adherence to the applicable export control regulations for its shipments even when it acts through freight forwarders or other agents. Accordingly, export compliance programs must involve designated personnel in shipping and receiving to ensure compliance. These individuals are the last line of defense to catch exports (or applicable imports) that may have missed compliance screening or been screened incorrectly. Some companies employ a fairly simple mechanism of training everyone in the shipping department to ensure that no export shipment leaves the facility unless it has been screened and has a sign-off by export compliance staff members, who complete a document such as an Export Compliance Checklist to signify their review and clearance of every export. If said document is not available, the shipping department may not release the shipment. Others involve the shipping department to a greater degree. The procedures set forth below are modeled after a company that involves its shipping department more heavily in

 bflowe@bcr-dc.com

export compliance.

Companies should designate certain individuals or the entire international shipping department with responsibility for ensuring completion of basic export clearance functions. In this section, those individuals and their backups are called export compliance officers and are trained by and work under the supervision of the export compliance administrator for these purposes as well as their direct line supervisor. The export compliance officers must ensure that each shipment complies with the export clearance requirements of EAR Part 758 and applicable sections of the ITAR and other applicable export control regulations.

The export compliance officers may not authorize release of any international shipment without some evidence of review by the export compliance staff that specifies the applicable export license and the ECCN (or Munitions List Category) so they will be able to complete appropriate documentation. This section assumes that export compliance staff complete the commercial invoice with required documentation to allow export compliance officers to complete properly the Automated Export System ("AES") record and the applicable transportation document (air waybill or bill of lading). Export compliance officers must be authorized to place a hold on any export shipments if they have any question as to their legitimacy until such questions are satisfactorily resolved by the export compliance administrator or other appropriate persons.

For U.S. exports (but not reexports), the export compliance officers must supervise the execution of an AES record for each shipment in accordance with the requirements of EAR § 758.3 as well as ITAR, Census Bureau, and Customs requirements. Filing deadlines under AES depend on which one of the four AES options is being used in a particular case.

A U.S. company's export compliance officers must complete AES records for the vast majority of exports including among others: (1) virtually all shipments (including hand carried items, since they constitute exports) valued at more than $2,500 (for non-mail shipments), (2) all shipments requiring an export license, and (3) all exports to destinations in Country Group E:1 (currently Cuba, Iran, North Korea, Sudan, and Syria). AES records must be filed before departure. In particular, they must ensure to designate the License Number or NLR or the License Exception Symbol or ITAR Exemption Reference (as applicable) on the AES record and ensure that it conforms with the one on the invoice and that it authorizes the export of the products listed therein. They shall also place the appropriate Schedule B (Harmonized Tariff Classification) numbers on the AES record for all products.

The U.S. company export compliance officers shall ensure that the Destination Control Statement, the ECCN for the highest level of controlled product (for example, 4A003, 4A994, EAR99), the License Number, NLR, or License Exception Symbol, and the value are placed on the commercial invoice, the AES record, and the bill of lading or air waybill (transportation document) accompanying each shipment. The EAR has one Destination Control Statement that may be used for all shipments. A Destination Control Statement is not required for reexports, but may be useful.

Many waybills supplied by freight forwarders will contain a preprinted Destination Control Statement and AES record information. Some freight forwarders complete the waybill and AES record on behalf of companies. In those cases, they must send records of the shipments back to the company, including copies of the AES record.

 bflowe@bcr-dc.com

The export compliance officers must also ensure that each shipment under their supervision otherwise complies with the Export Clearance requirements of EAR Part 758 and that the information on documents for License shipments conforms from document to document pursuant to the Rules of Conformity in EAR § 758.4(b).

There are special requirements for ITAR licensed exports, but they do not apply to reexports unless specified on a license. The District Director of Customs at the port of exit (or the Postmaster) must endorse the ITAR license prior to shipment. If for any reason the District Director does not endorse the license, the company's export compliance officer must self-endorse it. Licenses must be self-endorsed after technical data is transferred under the license to a non-U.S. person in the United States. (Often the technical data transaction is best addressed by the export compliance staff.) The export compliance officers must return the license to DDTC upon the earlier of completion of the export or expiration of the license. For exports of classified data or articles, DDTC will forward the export license directly to the Defense Investigative Service ("DIS") in accordance with the provisions of the DoD Industrial Security Manual, and will send the company an information copy. DIS will return the endorsed license to DDTC after the shipment. Exports of classified technical data must comply with the requirements of the DoD Industrial Security Manual.

For exports made pursuant to an ITAR exemption, the U.S. export compliance officer or his designee must certify that the export is exempt from licensing requirements by writing on the package or letter containing it, for technical data, "22 C.F.R. [insert applicable section]" identifying the specific ITAR section where the exemption is claimed. This certification must be made in written form and retained in the exporter's files for a period of five years. (ITAR § 125.6(a).)

The export compliance officers must ensure that the company retains copies of relevant shipping documents for at least five years. This includes copies of each of the commercial invoice, the AES record and the transportation document. Many companies do not routinely retain their AES records because they are provided to the freight forwarder, either separately or as a part of the forwarder's Shipper's Letter of Instructions or is a component part of the waybill. This is a mistake. The AES record is the legal document designating the appropriate compliance with U.S. export control laws. Also, many courier type freight forwarders complete AES records using information on the international waybill. If the freight forwarder completes one of thousands of AES records incorrectly, the company is responsible for this action of their agent. Accordingly, the company must be able to prove at minimum that the shipment left their loading document with correct paperwork. To be able to do that, the company must retain copies of applicable documentation. (I can provide forms of the required written assurances, which must be obtained, if applicable, in addition to standard company nondisclosure agreements.)

12.8. Recordkeeping and Reporting System.

Export compliance administrators should monitor the company's Recordkeeping system to ensure that it meets the requirements of EAR Part 762 and the special provisions referenced in Section 762.2. The Recordkeeping system may be flexible enough to allow for adaptations to updated Recordkeeping modes (*e.g.*, electronic or paper), but reproductions of original records must meet the strict requirements of EAR § 762.5. Recordkeeping should be consistent with the company's general Recordkeeping system. Records must be maintained for at least five years from the date of the last transaction to which they apply. These records must contain copies of

the following documents:

1. Standard operating guidance, legal memoranda and policy materials regarding export administration;

2. All correspondence with BIS, customers, and others regarding export administration;

3. Purchase orders, invoices, transportation documents, AES records, letters of special authorization, telexes, and any other correspondence with respect to each export transaction;

4. Logs of shipments made under NLR or License Exceptions LVS (to ensure compliance with the twelve shipment per year limitation) and TMP (to ensure return of temporary exports within one year);

5. Complete License Applications and Licenses with records of shipments made thereunder, amendments, and reexport applications;

6. International Import Certificates and other License supporting documents as required by EAR Part 775 (five years); and

7. Reports made to BIS under various reporting requirements.

BIS has placed increasing requirements for reporting on exports under License Exceptions in order to implement the Wassenaar Arrangement and for computer exports. While it has eliminated many of the reporting requirements for encryption exports, some significant reporting requirements still remain. Reports are reviewed by the Office of Export Enforcement, so exporters should take special care to ensure they comply with reporting requirements, and that reports are timely and accurate. *See* EAR Part 743.

12.9. Routed Export Transactions.

Often, a manufacturer or vendor in the United States will sell a product to a foreign customer with the latter's U.S. agent handling the actual exportation, including the assumption of export compliance responsibilities. These transactions are now known as "routed export transactions". Under the EAR, a U.S. seller will be treated as the exporter, and thus have export compliance responsibility, *unless* it obtains from the foreign customer a writing in which the latter expressly assumes this responsibility. A single writing can cover multiple transactions between the same parties. (EAR § 758.3(b).) U.S. export compliance administrators should implement procedures to ensure that such a writing is obtained from non-U.S. customers in cases in which the parties' intent is to shift export compliance responsibility to the foreign customer. They should also prepare a standard form that can be used for this purpose.

In routed export transactions, the U.S. manufacturer or vendor is required by EAR § 758.3(c) and § 30.3(c)(1) of the Foreign Trade Regulations ("FTR") to provide the foreign customer or its U.S. agent with the correct ECCN or sufficient technical information to classify the item. Also, under the same provisions, it must provide the foreign customer or its U.S. agent any information it knows will affect the licensing authority determination. The U.S. agent of the

 bflowe@bcr-dc.com

foreign customer must obtain a power of attorney or authorization from the latter to act on its behalf (EAR § 758.3(d)) and to file an AES record on its behalf (FTR § 30.3(c)(2)). While not required by the EAR, it would be a good practice for the U.S. manufacturer or vendor to obtain from the foreign customer's U.S. agent a copy of such power of attorney or authorization or at least to confirm that it has been obtained by the agent.

FTR § 30.3(c)(2) also requires the U.S. agent to provide the U.S. vendor or manufacturer, upon request, appropriate documentation verifying that the information provided by the U.S. vendor or manufacturer was accurately reported in the AES record. In such situations, the U.S. manufacturer or vendor should request the U.S. agent to provide it with actual copies of the AES record, even though the FTR allows the agent to satisfy this requirement by other means. It is important for the U.S. manufacturer or vendor to verify that the agent has completed the AES record accurately because the former will be listed as the "U.S. Principal Party in Interest" on the AES record, even though it is not treated as the exporter of record under the EAR. The party on the AES record formerly identified as "Exporter" is now be called "U.S. Principal Party in Interest". While designation on the AES record as the "U.S. Principal Party in Interest" in routed export transactions is supposed to be just for statistical purposes, exporters should be aware that export enforcement officials have in the past relied on information supplied in the AES record to determine the identity of the exporter and thus the party responsible for an export violation.

All parties are responsible for maintaining records with respect to what they have submitted to demonstrate export compliance. Section 10.10 discusses the BIS and Census Bureau exporter of record rules in more detail. The rules, particularly the BIS one, are very important regulations because of their effects on export liability, documentation, and other requirements.

12.10. Training of Personnel.

Because of the complexity of U.S. export control laws even with simplification, it is essential that each employee responsible for export compliance functions be instructed and receive refresher courses on export compliance guidelines. Those who are directly responsible for export compliance must receive the most in-depth training and refresher courses feasible. All other personnel involved in export related functions must also receive some compliance training.

In this connection, the following procedures are recommended training guidelines:

1. From time to time, as appropriate, the company's export compliance procedures manual should be updated and distributed to appropriate personnel, including particularly those responsible for its implementation. Likewise, an Export Compliance Policy Memorandum should be distributed annually by top management to all personnel involved in international sales and shipping that summarizes the compliance program, indicates the persons responsible for reviewing export transactions and the locations of the written procedures, and reaffirms the company's commitment to compliance with U.S. export control laws, as described above. Such a memorandum serves an important general employee training function.

2. Whenever a new employee is hired in an export related capacity, his/her immediate supervisor should include in his/her orientation a discussion of the export compliance program and the new employee's role in it. The same procedures should be followed for

 bflowe@bcr-dc.com

employees transferred from other departments. All new employees involved in sales, customer service, transportation, and shipping should receive a copy of the current Export Compliance Policy Memorandum in his/her orientation package.

3. From time to time, as determined appropriate by the export compliance administrator, he/she and others they select should attend outside seminars on export controls, including seminars on changes to the regulations and overall refresher courses. An in-house seminar conducted from time to time for export related personnel like this one is always helpful. Some time during audits should be devoted to training.

4. Training should cover all of the procedures required by the compliance program, as applicable for the particular employees.

5. After each annual internal audit, the export compliance administrator should consider calling a meeting of export related personnel to review procedures, explain improvements to be made, and obtain suggestions for improvements.

6. The export compliance administrator should also distribute periodic memoranda and other materials to responsible personnel on updates and revisions to the EAR, U.S. export policies, and company compliance procedures, including EAR subscriptions, BIS Newsletters, and legal guidance.

12.11. <u>Internal Audit System</u>.

On a regularly scheduled basis, if the company is not audited by one of its parent companies (or in addition), the General Counsel should designate a person who is knowledgeable about matters contained in the company compliance program but not affiliated with daily export functions to conduct a thorough audit of the export compliance program. The auditor may be either someone independent from the company or a company employee responsible to the General Counsel or the President and not subject to ultimate control by the export compliance administrator. The auditor should use as one reference the audit module/checklists distributed from time to time by the BIS. The export compliance administrator should shall also perform spot checks of operations from time to time.

Audits should include the following elements:

1. Flow charting the order processing system;

2. Obtaining product and customer information to identify focus of review;

3. Interviewing export-related personnel;

4. Inspecting all required export-related documents;

5. Analyzing sample transactions;

6. Reviewing the export compliance program, additional implementation guidelines, and comparing it with actual export compliance procedures;

 bflowe@bcr-dc.com

7. Confirming screening for Denial Lists, diversion risks, nuclear, missile, and chemical and biological weapons end-users/uses, and other required screening;

8. Reviewing customer and product lists to ensure that no parties on the Denial Lists or nuclear, missile or chemical or biological weapon parties are present and that the commodities in the Product Matrix have been correctly identified as eligible for NLR or License Exception shipments;

9. Reviewing any deviations from the procedures set forth in the written compliance program, including discrepancies between required procedures and actual procedures, unusual transactions, or violations of the EAR;

10. Verifying existence of the following export control documents:

    a. Copy of current EAR in a place available to the export compliance administrator, General Counsel, and other appropriate personnel, the CCL therein available to any engineers who perform export classifications, and Section 758 thereof available to the international shipping personnel;

    b. Updated Denial Lists, red flag indicators, and distribution thereof to all applicable personnel;

    c. All Licenses;

    d. International Import Certificates, Forms 629P, and other end-user supporting documentation for license applications;

11. Verifying the following records for export transactions:

    a. All shipping documents;

    b. All invoices, contracts, purchase orders, and the like; and

    c. Proper destination control statements, License Numbers or NLR or License Exception Symbols, ECCNs, and values in AES records, invoices, and waybills;

12. Verifying order processing as follows:

    a. Whether Export Compliance Checklists have been completed and other required screening performed as required by the export compliance program;

    b. Whether a Product Matrix is maintained and has been used properly;

    c. Whether company personnel are correctly following procedures for

 bflowe@bcr-dc.com

(i) processing orders to determine whether a NLR or License Exception or an License is appropriate for an export shipment, (ii) conducting Denial Lists reviews, (iii) conducting diversion risk screening, (iv) conducting nuclear, missile and chemical and biological weapons end-users/uses screening, and (v) routing all export shipments through designated compliance personnel to ensure screening;

13. Verifying the following export compliance program documentation:

    a. The existence of the written export compliance program and its availability to requisite personnel, appropriate updates hereto, and current names and functions of personnel assigned compliance duties;

    b. Current lists of persons who are responsible for administration of the program;

    c. Training records; and

    d. Methods for addressing deficiencies or problems.

Each auditor shall be adequately trained to perform these audit functions.

After each audit, the designated auditor should prepare a report to the General Counsel summarizing his/her findings on the company's adherence to its own compliance program and the law with a list of action items to be accomplished. The General Counsel should present a summary and his reaction to it to the President. Upon instruction by the General Counsel, the export compliance administrator should take all appropriate steps to correct any deficiencies encountered and to improve the functioning of the compliance program.

12.12. Policy for Addressing Compliance Problems.

No one is perfect. Any company that makes substantial export shipments will experience problems from time to time in complying with complex U.S. export control laws and regulations. That is why companies establish compliance programs in the first place. Therefore, it is essential to establish procedures to handle any problems that arise, including suspected violations or deviations from procedures as well as judgment calls that involve any risk to the company. A controlled mechanism for handling problems will help a company respond to them quickly and systematically. This element also is part of senior management's demonstration of a commitment to compliance. Many companies that decide to make voluntary disclosures to authorities can do more harm than good by making them too quickly before developing knowledge of the essential relevant facts (absent an incipient threat that can be halted by enforcement agencies).

Each company will wish to develop problem solving policies and procedures in accordance with its own style of doing business and delegating decision-making authority within the company. The suggested procedures described herein assume that the General Counsel of the company (or other appropriate management official) supervises legal compliance issues and

 bflowe@bcr-dc.com

should therefore be consulted on any non-routine legal issues. Generally, companies will want to establish a hierarchy so that routine questions are handled by day-to-day compliance staff, but that non-routine judgments and any questions of illegality are referred to the export compliance administrator and further to the legal counsel, perhaps with other levels of review in between. Compliance staff will often have the best judgment on what actions to take, but should be encouraged to share the risks of their judgment calls with their supervisors absent established policies and procedures for handling particular problems.

An exporting company should consider inserting a statement along the following lines in its manual and a shorter version in its statement of compliance policy:

> Any employee having a reason to know of a deviation from the policies or procedures prescribed by this manual shall immediately bring the matter to the attention of the export compliance administrator. This includes any potential violations of the EAR, ITAR, or other export controls with respect to company shipments, any evidence of export violations by customers, resellers, or distributors, any failure to fulfill the procedures required by this export compliance manual, and reports by U.S. government officials. The export compliance administrator shall immediately bring any such matter to the attention of the General Counsel and take appropriate steps to halt any potentially offending shipment. If the problem requires prompt action to prevent U.S. national security or foreign policy risks (such as high technology falling into the hands of a party that poses a serious threat), the compliance administrator and General Counsel shall take immediate steps to prevent the problem from occurring, including promptly reporting it to cognizant government agencies. Otherwise, the compliance administrator shall promptly investigate the matter and follow up the initial report to the general counsel with explanations, if any, of the matter.

The export compliance administrator, under the supervision of the General Counsel, should conduct an immediate investigation of each such compliance report. After consultation with the General Counsel, the export compliance administrator and/or the General Counsel should take appropriate action, which may include a report of the matter to BIS, DDTC, or other appropriate government officials.

The export compliance administrator and his/her designees should seek appropriate guidance from BIS or other sources to clarify export licensing and compliance requirements.

Company counsel should also prepare appropriate contracting terms and other notices to assist the company in export compliance. For example, companies should include appropriate contingency or *force majeure* clauses in sensitive export sales contracts to avoid delivery penalties or liability for licensing delays, restrictions on performance imposed on licenses, denials of licenses, and future amendments to U.S. export control laws and regulations that may inhibit delivery, servicing, warranty performance, and software updates. Methods for resolving issues arising from license provisos or conditions imposed by government agencies should also be considered for large contracts for sensitive items, especially those for sales to countries of special export control sensitivity.

Company counsel should also consider inserting specific export compliance requirements in contracts with distributors and resellers who either are authorized to sell outside their home

 bflowe@bcr-dc.com

countries or are located in countries listed in Country Group D (Supplement No. 1 to EAR Part 740).

Finally, written assurance provisions against reexport of technologies or the direct product thereof should be included in licensing agreements to comply with License TSR requirements discussed above. Special versions of nondisclosure agreements containing these written assurances are appropriate for nonimmigrant personnel.

13. Current and Expanded Issues of Particular Interest.

13.1. The Administration's Export Reform Initiative.

The Obama Administration Export Control Reform Initiative is focused on 4 key areas, the so-called "Four Singles" – A Single Enforcement Agency, Single Information Technology System, Single Licensing Agency and, of most immediate significance, a Single Control List.

Progress toward a Single Enforcement Agency took a big step forward in March of 2012 when the Export Enforcement Coordination Center (aka, E2C2) became operational. The purpose of the Enforcement Center is to enhance coordination and information sharing among the many agencies, across several administrative departments, that have some involvement with export control enforcement. The opening of the Enforcement Center is said to have greatly expanded efficiency in enforcement matters, though this may not be immediately apparent to the exporting public.

The Administration continues the progress of migration to a Single Information Technology ("IT") System from at least three different legacy systems. The process of interagency review of export licenses is being moved to a single IT platform, USXports, a system previously used only by the Defense Department. This change is really just a "back-end" improvement visible only to the agencies involved in export control (but notably excluding the Office of Foreign Assets Control, Nuclear Regulatory Commission and Department of Energy). The only benefit to the exporting public is the increase in efficiency that should result when DDTC and BIS are using the same system. DDTC has already completed its migration to the new system. While target completion for the BIS migration was expected already, due to mandatory cuts resulting from 2013 sequestration and a government shutdown, BIS has had to place its USXports reconfiguration on hold for the time being. Hopefully the delay will not be for much longer.

BIS has also recently launched three new online "decision tree" tools on Export Control Reform topics: The CCL Order of Review Tool, the Specially Designed Tool, and the License Exception STA Tool. Each of the tools takes the user through a list of yes or no questions leading to a conclusion, in a "decision tree" or flow chart like structure. The Order of Review Tool is, like its name suggests, a tool to assist the user in jurisdiction and classification determinations. The specially designed tool provides a more straightforward and user-friendly question and answer analysis of the new definition of the term, discussed below, than resorting directly to the definition itself. The License Exception STA Tool, similarly, guides the user through a series of questions and answers to determine whether a given transactions is eligible for License Exception STA. We found the STA Tool to be the most useful of these tools (with the Specially Designed Tool a close second), because it eliminates some of the need to flip back

 bflowe@bcr-dc.com

and forth between different sections in the EAR and also ensures that no restrictions on use of License Exception STA are overlooked. All of them are addressed.

Additional IT improvements to look forward to will likely be in the form of an online submission form to report boycott requests, and a single registration process and platform for submitting license applications online (as opposed to BIS's SNAP-R and DDTC's D-TRADE online license application platforms). As President Obama has been reelected, we are fairly optimistic that these IT reforms will be implemented during his second term.

The Single Licensing Agency seems to have been given last priority relative to the other reform areas. This is primarily because movement to a Single Licensing Agency will require legislative action and the Administration realizes progress here is unlikely in the short term with a Republican controlled House of Representatives. Moreover, Hill staffers have more than enough to focus on with the massive overhaul of the control lists that is currently underway. Given that there is relatively little the Administration can do to advance this through administrative action alone, any progress here will be slow in coming.

However, in the short term the Administration is trying to harmonize some of the licensing practices and license exceptions under the Export Administration Regulations ("EAR") and International Traffic in Arms Regulations ("ITAR"). Although the EAR is generally more flexible and less restrictive than the ITAR, there are a few instances where this is not so, primarily in the context of license duration, and of certain ITAR license exemptions that either did not exist, or were more narrowly construed, under the EAR. To address this, in its new final rule BIS, discussed in detail below, is lengthening the validity period for EAR licenses from two years to four years (or longer on a case-by-case basis), and is revising the provisions of several EAR license exceptions to make them more consistent with the analogous ITAR provisions.

The Administration has made the most progress in its work toward a Single Control List. The Administration has been pursuing reform that would make the USML and CCL more positive lists of specifically enumerated items, and more aligned so that eventually they can be combined into a Single Control List. By "positive list" we mean a list that describes controlled items using objective criteria rather than broad, open-ended, subjective, or design intent-based criteria. Also, the Administration has been trying to create a bright line between the USML and the CCL to reduce jurisdictional uncertainty. The Administration had also initially intended to divide the control lists into three tiers, or levels of controls (i.e., least restrictive, more restrictive, most restrictive), but has decided to defer its efforts at tiering for now so it could focus more on reforms that can be implemented in the near future and that would make the lists more positive in nature. The first major steps of control list reform, moving items from the USML to the CCL, have just begun, as discussed in the next sections.

13.2. The First Final Rules.

On April 16, 2013, BIS and DDTC published the first final rules moving items from the USML to the CCL. 78 *Fed. Reg.* 22660 (Apr. 16, 2013) and 78 *Fed. Reg.* 22740 (Apr. 16, 2013) (the "BIS Final Rule" and the "DDTC Final Rule," respectively). We affectionately refer to these rules as the "Beast" and the "Baby Beast" due to their length and exhaustive level of detail. As the length of the ITAR relative to the EAR would suggest, the DDTC Final Rule was the least painful to wade through, while the BIS Final Rule was gargantuan in scope and labyrinthine in its organization, just like the EAR itself, because the EAR provides more rules for exporters to self

apply. While we touch on some of the most fundamental and generally applicable parts of the final rules, a full and complete explanation of them is beyond the scope of this memorandum. We suggest that at least one knowledgeable individual (if not all senior compliance personnel) in every organization go through the painstaking task of a careful reading of the final rules in order to fully ascertain the implications for the organization. Simply put, the rules can only be summarized to a degree, and nothing will substitute for a thorough reading by senior compliance personnel familiar with the organization's products and current processes and internal controls and applying them to reclassification of items and revision of export compliance procedures.

13.2.1. Ground Rules to Ease the Transition. In addition to moving the first tranche of items from the USML to the CCL, the DDTC and BIS Final Rules explained in great detail some very important ground rules for the next steps of the transition, which we summarize here. The movement of items from the USML to the CCL is discussed below.

First, all final rules will have a 180-day transition period before implementation. During this period, BIS will begin accepting and reviewing license applications for the items moving from the USML to the CCL but will not issue licenses until after the effective date. DDTC will also accept license applications for such items during the 180-day transition period.

Second, a DDTC-issued license for items transitioning to the CCL that is issued prior to the effective date for the relevant USML category, and that does not include any items that will remain on the USML, will remain valid until expired, returned by the license holder, or for a period of two years from the effective date, whichever comes first. If only some of the items listed on the license have transitioned to the CCL, the DDTC-issued license will be valid for all of the items through its expiration date. Any temporary licenses (e.g., DSP-73) that are issued in the period prior to the effective date for the relevant USML category will remain valid until expired or returned by the license holder.

Third, a new ITAR § 120.5(b) will provide for a mechanism whereby DDTC can license export of certain items moved to the CCL and that are thus "subject to the EAR." Each revised USML category as it is finalized will have a new subcategory (x) for items "subject to the EAR," provided the items will be used in or with defense articles controlled on the USML, and provided the items are described in the purchase documentation submitted with the license application. DDTC will begin to accept license applications citing a new subcategory (x) entry once the 180-day transition period has passed for the related USML category. This will eliminate the need to seek a separate license from BIS for exports of both ITAR-controlled and EAR-controlled items that will be used together abroad. If DDTC receives license applications for items that have transitioned to the CCL after expiration of the 180-day transition period, and the license application does not cite the new subcategory (x), the applications will be Returned Without Action with instructions to contact BIS.

Fourth, agreements and amendments containing both USML and CCL items will be adjudicated up to the effective date of the relevant final rule. Agreements including both transitioning and non-transitioning items that are issued prior to the effective date of the relevant final rule will remain valid until expired, unless they require an amendment, or for a period of two years from the effective date of the relevant final rule, whichever comes first. In order for an agreement to remain valid beyond two years, an amendment must be submitted to authorize the CCL items using the new subcategory (x) designation from the relevant USML category. Agreements including only transitioning items that are issued prior to the effective date of the

 bflowe@bcr-dc.com

relevant final rule will remain valid for two years from the effective date of the relevant USML category. After that, any ongoing activity must be authorized by BIS.

Fifth, previously issued Commodity Jurisdiction ("CJ") determinations for items deemed subject to the EAR will remain valid. CJ determinations for items deemed to be classified on the USML but that subsequently transitioned to the CCL pursuant to a final rule will be superseded by the final rule. Exporters who are certain that their items have transitioned to the CCL are encouraged to review the appropriate Export Control Classification Number ("ECCN") to determine the classification of their items, and if there is any doubt, to request a CJ from DDTC and/or a classification from BIS.

Sixth, parties registered with DDTC as manufactures, exporters, or brokers of defense articles/services are supposed to notify DDTC in writing if none of their business will involve defense articles/services after the transition of items from the USML to the CCL. Instructions for providing the notification are available on the DDTC website (www.pmddtc.state.gov). The registrations will not be canceled or revoked, but just permitted to expire (sorry, no partial refunds). If a party will no longer have business involving defense articles/services after the effective date of the relevant final rule, but their registration will expire *before* the effective date, they can request that DDTC extend their existing registration and they will not be charged a new registration fee.

13.2.2. The "600 Series". Once the final rules are fully implemented, the items moved from the USML to the CCL will be housed in new "600 Series" (XX6XX) ECCNs. The 600 Series will also include Wassennar Arrangement Munitions List items currently classified under existing XX018 ECCNs. Paragraph .x of the 600 Series ECCNs will control parts, components, accessories and attachments specially designed for the end-items in the 600 Series ECCNs or for defense articles in the USML and not elsewhere specified on the USML or the CCL. Paragraph .y will control specific enumerated parts, components, accessories and attachments that, although specially designed for a defense article or 600 Series end-item, warrant no more than Anti-terrorism ("AT-1") controls because they are so militarily insignificant. BIS had proposed to also create a paragraph y.99 to house items that had been determined in a CJ ruling to be subject to the EAR and for which, at least prior to the creation of the 600 Series, were not enumerated on the CCL. However, BIS decided against this proposal and did not adopt it in the recent final rule, deciding that such items should retain their EAR99 status if not otherwise identified on the CCL.

The 600 Series ECCNs generally would be subject to National Security ("NS-1"), Regional Stability ("RS-1") and AT-1 controls, except for the .y paragraphs, which would only be subject to AT-1 controls. Accordingly, other than paragraph .y, a license would be required for export to all destinations except for Canada. Some 600 Series items would be subject to additional reasons for control, such as chemical and biological weapons reasons ("CB-1"), in which case a license would be required for all exports, even to Canada. All exports other than .y items to countries subject to a U.S. arms embargo would be subject to a general policy of denial (as is the case now under the ITAR), unless they meet the narrow carve-outs described in ITAR 126.1. See discussion below on prohibition on exporting .y items to China.

13.2.3. License Exceptions. The major benefits of the transfer from the USML to the CCL would be that certain license exceptions and/or the *de minimis* U.S. content rule would

 bflowe@bcr-dc.com

be available in some cases to authorize transfers. Limitations on use of License Exceptions for the 600 Series ECCNs are now set forth in EAR 740.2.

The BIS Final Rule will revise provisions of several License Exceptions to make them more consistent with the analogous ITAR provisions. For example, the BIS Final Rule (once fully implemented) will revise License Exception TMP to allow temporary exports to any U.S. subsidiary or affiliate abroad, not only those located in Country Group B, because the ITAR exemption for temporary exports does not have such a limitation. Similarly, the BIS Final Rule will expand License Exception GOV to allow, in certain circumstances, exports to non-governmental end-users acting on behalf of the U.S. Government, such as U.S. Government contractors, and to incorporate provisions consistent with ITAR 125.4(b)(1), (b)(3), and 126.6(a), concerning certain exports made at the direction of the Defense Department. License Exception TSU will be revised to allow U.S. universities to release software and technology to their foreign national employees in the United States, and to allow export of copies of technology previously authorized for export to the same recipient, similar to the exemptions found at ITAR 125.4(b)(10) and (b)(4), respectively. A number of other more technical conforming changes will also be made once the BIS Final Rule is implemented, but these are some of the highlights.

The BIS Final Rule will also make several changes to License Exception STA. License Exception STA generally will be available for eligible end-items if, at the time of export, reexport or transfer (in-country) the item is destined: (i) for ultimate end-use by the U.S. Government or by the armed forces, police, paramilitary, law enforcement, customs, correctional, fire, and search and rescue agencies of a government in one of the 36 countries in EAR 740.20(c)(1), now comprising a new Country Group A:5, or (ii) for the "development" or "production" of an item for ultimate end-use by any of the said foreign government agencies in any of the A:5 countries, by the U.S. Government, or by any person in the United States. Exports and reexports under License Exception STA to non-governmental end-users in one of the A:5 countries would be permissible so long as the item at issue would be ultimately provided to, or for the production or development of an item to be provided to and for end-use by, any of the foregoing agencies of an A:5 government, the U.S. Government, or any person in the United States.

Note that License Exception STA may not be used for any 600 Series items identified in the relevant ECCNs as ineligible for export under STA. It also may not be used to export end-item aircraft classified in ECCN 9A610.a until after BIS has approved their export under STA under new procedures set forth in EAR § 740.20(g).

The BIS Final Rule will also limit use of License Exception STA for 600 Series items only to foreign parties that have received U.S. items under a license issued by BIS or DDTC. BIS licenses will be required for foreign parties who have not been previously approved under a BIS or DDTC license even if STA otherwise would be available. Certain other limitations, terms and conditions, such as special 600 Series consignee statement provisions, will also apply to the use of License Exception STA, as fully detailed in EAR 740.20.

13.2.4. The *De Minimis* and Direct Product Rules. BIS had initially proposed to subject 600 Series items to a 10% *de minimis* rule, meaning that foreign-made items incorporating any more than 10% of U.S.-origin 600 Series content would require a license from BIS for reexport. However, other items subject to the EAR are only subject to a 25% *de minimis* rule (unless destined to a terrorist supporting country, in which case the level is 10%). A number

 bflowe@bcr-dc.com

of comments submitted to BIS objected to having two different *de minimis* levels applicable to different items going to the same country. The reexporter/exporter from abroad would essentially have to perform two separate *de minimis* calculations for the different content, and it could become very cumbersome in application. To address this, the Final Rule established a uniform *de minimis* level of 25% for 600 Series items, consistent with that applicable to other items subject to the EAR, *provided* that the foreign-produced item is *not* being reexported to a country subject to a U.S. arms embargo. If the item would be reexported/exported from abroad to an arms embargoed country, no *de minimis* rule would apply, and a license thus would be required for any U.S. origin 600 Series content.

The BIS Final Rule also expanded the "direct product rule" to require a license for reexport/export from abroad of foreign-produced direct products of U.S.-origin 600 Series technology/software to arms embargoed countries, in addition to countries of concern for national security, chemical and biological weapons, missile technology, or anti-terrorism reasons (i.e., Country Groups D:1, D:3, D:4 and E:1).

13.2.5. The China Military End-Use Rule. The BIS Final Rule will subject all 600 Series items to the so-called "China Military End-Use" rule, thus establishing a license requirement for the export/reexport of all 600 Series items to the People's Republic of China ("China"). BIS reasoned that because all 600 Series items were specially designed for a defense article (or they would not be in the 600 Series in the first place), all such items are presumptively for a military end-use, and should therefore require a license for export/reexport to China, even paragraph .y items that are subject only to AT controls. This could be a trap for the unwary, as ordinarily items like those in paragraph .y that are only subject to AT controls do not require a license for export/reexport to China, and the ECCNs only indicate that AT controls apply.

Applications for exports/reexports to China will be reviewed on a case-by-case basis to determine whether they would make a material contribution to China's military, in the same manner as other China Military End-Use license applications are currently reviewed.

13.2.6. The New Definition of Specially Designed. Perhaps of greatest consequence is the new final rules' definitions of "specially designed." The concept is hugely important because it will still dictate to some extent whether certain items are subject to the ITAR or the EAR. Two earlier proposed definitions had been published, first by DDTC in December 2010 (75 *Fed. Reg.* 76935 (Dec. 10, 2010)), and next by BIS on July 15, 2011 (76 *Fed. Reg.* 41958 (July 15, 2011)). Since those earlier proposals, DDTC and BIS received and reviewed many comments on the topic and have reviewed the definition extensively with BIS's Technical Advisory Committees, in which Ben participates, and DDTC's Defense Trade Advisory Group. Even more comments were submitted in the wake of the June 19 proposed rules.

Both the DDTC and BIS definitions are similar but not identical. Like the earlier proposals, the final definitions employ a "catch and release" approach. That is, the first part of the definitions articulates a very broad scope for the meaning of "specially designed" – the "catch" – and then the second part of the definitions provides some exclusions from that scope – the "release." The definitions are intended to lead the reader through a "decision tree" type of analysis of yes/no questions leading to a more objective conclusion as to whether a given item is or is not specially designed. In this way, it is hoped that the new definitions will provide a relatively simple and straightforward approach to what can be a very complicated issue.

 bflowe@bcr-dc.com

However, as many in the trade community have expressed, the devil is in the details and the "simple" catch and release approach is not so simple in application, and the definitions are very lengthy, with several steps in the interpretive process.

Each of the definitions begin with some introductory text to briefly explain the sequential steps for application. Essentially, there are two parts to paragraph (a) of the definitions that broadly define items that are specially designed, and if any of them apply to the item in question, you continue to paragraph (b) of the definitions, each of which sets forth several exclusions. If none of the parts of paragraph (a) describes the item in question, then there is no need to proceed through to paragraph (b).

The final BIS definition (excluding numerous detailed explanatory notes) is as follows:

> When applying this definition, follow this sequential analysis set forth below. For additional guidance on the order of review of "specially designed," including how the review of the term relates to the larger CCL, see Supplement No. 4 to Part 774 – Commerce Control List Order of Review.
>
> (a) Except for items described in (b), an "item" is "specially designed" if it:
> (1) As a result of "development" has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant ECCN or U.S. Munitions List (USML) paragraph; or
> (2) Is a "part," "component," "accessory," "attachment," or "software" for use in or with a commodity or defense article 'enumerated' or otherwise described on the CCL or USML.
>
> (b) A "part," "component," "accessory," "attachment," or "software" that would be *controlled* by paragraph (a) is not "specially designed" if it:
> (1) Has been identified to be in an ECCN paragraph that does not contain "specially designed" as a control parameter or as an EAR99 item in a commodity jurisdiction (CJ) determination or interagency-cleared commodity classification (CCATS) pursuant to § 748.3(e);
> (2) Is, regardless of 'form' or 'fit,' a fastener (e.g., screw, bolt, nut, nut plate, stud, insert, clip, rivet, pin), washer, spacer, insulator, grommet, bushing, spring, wire, solder;
> (3) Has the same function, performance capabilities, and the same or 'equivalent' form and fit, as a commodity or software used in or with an item that:
> (i) Is or was in "production" (i.e., not in "development"); and
> (ii) Is either not 'enumerated' on the CCL or USML, or is described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
> (4) Was or is being developed with "knowledge" that it would be for use in or with commodities or software (i) described in an

 bflowe@bcr-dc.com

ECCN *and* (ii) also commodities or software either not 'enumerated' on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled ony for Anti-Terrorism (AT) reasons;

(5) Was or is being developed as a general purpose commodity or software, i.e., with no "knowledge" for use in or with a particular commodity (e.g., an F/A-18 or HMMWV) or type of commodity (e.g., an aircraft or machine tool); or

(6) Was or is being developed with "knowledge" that it would be for use in or with commodities of software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) exclusively for use in or with EAR99 commodities or software.

The final DDTC definition is substantively very similar, except that it uses the term "commodity" when the term "item" is used in the BIS definition, and it only refers to the USML, as opposed to both the CCL and USML. There are a few other differences necessitated by some other inconsistencies between the conventions and nomenclature used in the CCL and USML, but the definitions are intended to be interpreted consistently. (BIS also believes that its definition is consistent with that found in the Missile Technology Control Regime, although most exporters would prefer the narrower MTCR version.) Finally, the ITAR definition does not have part (b)(6), which thus applies only to EAR items. Both definitions also have a number of lengthy explanatory notes that are not entirely identical but, again, not inconsistent. For example, both definitions feature an explanatory note defining the word "enumerated" as it is used in the definitions, but the BIS definition of enumerated is longer and provides more explanation and an example.

Both definitions limit paragraph (a)(1) with the phrase "if, as a result of "development." The DDTC rule defines "development" as "related to all stages prior to serial production, such as design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts." Thus, an item is only "caught" in the first part of the analysis if someone engaged in any of these "development" activities with respect to the item in question. Accordingly, the DDTC Final Rule suggests asking these question to help determine whether an item is captured: Does the item, as a result of "development" have properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described? If no, the item is not specially designed. If yes, then the next step of the analysis would be to consider whether any of the exclusions in part (b) apply. Part (b) is intended to reinforce the principles in ITAR § 120.3 that an item should not be ITAR-controlled if it has a predominant civil application or a civil performance equivalent, unless it nonetheless provides the United States with a critical military or intelligence advantage.

Suffice it to say that, due to the sheer length of the definitions, it will likely take a lot of practice and numerous applications to specific facts before any one person will be able to internalize the definitions and apply them without a painstaking line-by-line reading. However, even with its shortfalls, the new definitions arguably will be much preferable to the status quo of no definitions and inconsistent interpretations by DDTC and BIS of ITAR 120.3 in its current form.

 bflowe@bcr-dc.com

13.2.7. Rubric for Jurisdictional Analysis Under the Final Rules.

You may be wondering, where does all of this leave me, and how do I make sense of this new jurisdictional paradigm? We have devised what we hope will be a quick reference interpretive guide, or rubric for jurisdictional analyses going forward. When considering whether a particular item is subject to the ITAR or EAR, go through these steps:

1. Is this item enumerated on the USML? If yes, the item is ITAR-controlled. If no, proceed to step 2. (Note that you should only apply the definition of "specially designed" if those words appear in the relevant USML entry you are considering.)
2. Is this item enumerated on the CCL? Look first to the 600 Series if the item is one that was (or may have been) formerly on the USML and then to the rest of the CCL. If yes, proceed to step 3. If no, your item is EAR99.
3. Review the provisions of the EAR License Exceptions and determine whether any apply.

The ITAR definition of "specially designed" will only apply to USML Categories that have been revised, whereas the EAR version will apply wherever the words are used other than for MTCR items.

13.3. Final and Proposed Control List Changes to Date.

Considerable progress has been made on control list reform. To date, two final rules have just been published that, once fully implemented on October 15, 2013, will move many items from the USML to the CCL, and proposed rules have been published for about half of the remaining USML categories. For the remaining categories, proposed rules have been drafted but not yet published, as they are awaiting review by the Office of Management and Budget. The USML categories yet to be addressed in proposed or final rules are the following:

- Category I (Firearms)
- Category II (Guns)
- Category III (Ammunition)
- Category XII (Sensors)
- Category XIV (Chem/Bio Agents)
- Category XVIII (Directed Energy Weapons)

(No specific items are enumerated in USML Categories XVII (Classified Items) and XXI (Miscellaneous), so there is nothing to remove to the CCL for those categories.) What remains to be addressed are the categories that will probably see the least amount of change because they are where weapons and weapons systems are classified. Note, however, that the 2013 National Defense Authorization Act has paved the way for the Administration to move commercial satellites from the USML.

 bflowe@bcr-dc.com

13.3.1. Final Rules Regarding Military Aircraft. On April 16, 2013, DDTC issued a final rule to revise USML Category VIII (aircraft and related articles) (78 *Fed. Reg.* 22740 (Apr. 16, 2013)) to remove items that do not warrant control on the ITAR and to create a more positive list of items controlled by Category VIII. Also on April 16, 2013, BIS issued a final rule to describe how the items removed from USML Category VIII would be controlled under the EAR. (78 *Fed. Reg.* 22660 (Apr. 16, 2013)).

As explained in the Preamble to BIS's *proposed* rule on Category VIII, the U.S. Government will decide if an item should remain on the USML or move to the CCL as follows:

> The review was focused on identifying the types of articles that are now controlled by USML Category VIII that are either (i) inherently military and otherwise warrant control on the USML or (ii) if it is a type common to civil aircraft applications, possess parameters or characteristics that provide a critical military or intelligence advantage to the United States, and that are almost exclusively available from the United States. If an article satisfied one or both of those criteria, the article remained on the USML. If an article did not satisfy either standard but was nonetheless a type of article that is, as a result of differences in form and fit, 'specially designed' for military applications, then it was identified in the new ECCNs proposed in this notice.

This same model was used in deciding if an item should remain in the other USML categories as well.

13.3.1.1. Summary of Final DDTC Rule on USML Category VIII. The main change that was made by the DDTC Final Rule was the removal of ITAR controls on many generic aircraft parts, components, accessories, and attachments that are specifically designed or modified for a defense article. According to Eric Hirschhorn, Under Secretary for BIS, when assessing the changes to the USML, he believed the changes to USML Category VIII would probably have the biggest impact. Jurisdiction over the majority of parts and components that DDTC authorized in recent licenses will be transferred from the ITAR to the EAR as soon as the final rules are fully implemented on October 15. The new rule will not decontrol all parts and components. Parts, components, accessories, and attachments "specially designed" for the following aircraft are still covered on the USML: B-1B, B-2, F-15SE, F/A-18 E/F/G, F-22, F-35, and future variants thereof, or the F-117 or U.S. Government technology demonstrators. Paragraphs (h)(2)-(h)(26) also identify a number of other specific parts and systems still subject to controls, such as "wing folding systems and specially designed parts and components therefor," and "threat adaptive autonomous flight control systems." However, all other parts, components, etc., specially designed for military aircraft fall under the new 600 Series controls in Category 9 of the CCL.

The DDTC Final Rule also narrowed the types of aircraft subject to the USML, provided a revised definition of "aircraft," and moved certain items from USML Category VIII

into a new Category XIX for gas turbine engines. Finally, the final rule creates a new subcategory VIII(x) allowing for DDTC licensing of items "subject to the EAR" if the items are to be used with items in USML Category VIII and are described in the purchase documents submitted with the license application. This will prevent the need to seek licenses from both BIS and DDTC, where applicable.

13.3.1.2. Summary of Final BIS Rule on Military Aircraft. The BIS Final Rule, once fully implemented, will create five new ECCNs (i.e., 9A610, 9B610, 9C610, 9D610, and 9E610) to control the items removed from USML Category VIII. The rule also will move items currently classified under ECCNs 9A018, 9D018, and 9E018 to the new 600 Series ECCNs.

The BIS Final Rule will delete as obsolete EAR § 770.2(i) Interpretation 9: Civil aircraft and Civil aircraft equipment (including parts, accessories, attachments, components, and related training equipment).

The new 600 Series aircraft ECCNs will cover certain aircraft, ground equipment, aircrew life support and safety equipment, and certain military aircraft instrument flight trainers, among other things. The .y paragraph includes a long list of miscellaneous items such as aircraft tires, check valve filters, lavatories, and life rafts. These items will be subject only to AT controls. As customary in the CCL, certain related test, inspection and production equipment, and certain materials, software and technology will also be controlled.

13.3.2. Final Rules Regarding Military Engines. On April 16, 2013, DDTC issued a final rule that will create a new USML Category XIX for engines, populating it with engines and engine parts currently classified in USML categories VI (Vessels of War and Special Naval Equipment), VII (Tanks and Military Vehicles), and VIII (Aircraft and Associated Equipment), and removing other military gas turbine engines and related items from the USML. (78 *Fed. Reg.* 22740 (Apr. 16, 2013)). On the same day, BIS issued a final rule to describe how the items removed from the USML would be controlled under the EAR. (78 *Fed. Reg.* 22660 (Apr. 16, 2013)). The final rules on military engines were published as part of the same final rules cited above addressing military aircraft.

13.3.2.1. Summary of Final DDTC Rule on USML Category XIX. The main change made by the DDTC Final Rule is the removal of ITAR controls on certain military engines and engine parts, components, accessories, and attachments that are specifically designed or modified for a defense article. The intent of the new category is to make it clear that military gas turbine engines meeting certain objective parameters, regardless of the application, whether it be cruise missiles, surface vessels, vehicles and aircraft, are controlled on the USML, and to house them all in one specific category, while also removing certain items not warranting ITAR controls.

There are a few changes between the final rule and the proposed rule, based on comments submitted to DDTC. For example, some of the parameters distinguishing military from

 bflowe@bcr-dc.com

commercial capabilities were changed and the description of "hot section" components in subcategory XIX(f)(2) was revised so as to avoid inadvertently expanding the controls on them.

13.3.2.2. Summary of Final BIS Rule on Military Engines. The BIS Final Rule, once implemented, will create five new ECCNs (i.e., 9A619, 9B619, 9C619, 9D619, and 9E619) to control the gas turbine engines and related items removed from USML Categories VI, VII, and VIII. The rule also will move military trainer aircraft turbo prop engines and related items from ECCNs 9X018 to the new 9X619 series ECCNs. Consistent with the approach in the DDTC Final Rule, BIS's final rule will consolidate all military gas turbine engines (for aircraft, ships, and vehicles) into a single ECCN, 9A619.

The new ECCNs essentially will cover certain military gas turbine engines, engine controls, certain hot section components and other parts, components, accessories and attachments, along with test, inspection and production equipment therefor, and certain materials, software and technology therefor. Several specific items were enumerated in paragraph .y, subject only to AT controls, such as oil tanks and reservoirs, oil lines and tubes, fuel and oil filters, and shims.

13.3.3. Final Changes Regarding Military Vehicles. On July 8, 2013, DDTC issued a final rule to revise USML Category VII. 78 *Fed. Reg.* 40922 (July 8, 2013). Also on July 8, 2013, BIS issued a final rule to describe how the items removed from USML Category VII will be controlled under the EAR. 78 *Fed. Reg.* 40892 (July 8, 2013).

Once implemented on January 6, 2014, the final rule will move approximately 90% of the current contents of the category to the CCL, so will have far-reaching consequences.

13.3.3.1. Summary of Final DDTC Rule on USML Category VII. While the final rule continues use of the term "specially designed," it established much more objective criteria to determine if an item is controlled by Category VII. Many military vehicle parts, components, accessories, and attachments that are specifically designed or modified for a defense article will be removed from ITAR controls, as will some military vehicles. The final rule also provides a detailed definition of ITAR-controlled "ground vehicles." Experts estimated that some 75% of items should move to the EAR because few were viewed as providing a critical military function.

13.3.3.2. Summary of Final BIS Rule on Military Vehicles. Under its final rule, BIS revised five ECCNs (i.e., 0A606, 0B606, 0C606, 0D606, and 0E606) that BIS first proposed on July 15, 2011. Under BIS's final rule, ECCN 0A606.a will control ground vehicles "specially designed" for a military use and not enumerated in USML Category VII. ECCN 0A606.b will control other ground vehicles, and certain listed parts and components. ECCN 0A606.b.1 would control unarmed vehicles derived from civilian vehicles that have been modified or fitted with materials or components (other than reactive or electromagnetic armor to provide ballistic protection to level III or better), and meeting certain other specified parameters, and ECCN 0A606.b.2 will control parts and components that provide ballistic protection to level III or better "specially designed" for ground vehicles controlled by ECCN 0A606.b.1.

Under the final rule, the vehicles and parts and components in ECCN 0A606.b would be subject to National Security 2 ("NS-2"), Regional Stability 2 ("RS-2"), Antiterrorism 1 ("AT-1"), and United Nations ("UN") reasons for control. This will allow the items to be exported to most NATO member countries, Australia, New Zealand, and Japan without a license.

The final rule will remove Interpretation 8: Ground Vehicles in EAR § 770.2(h) on the grounds that it would no longer be necessary. The final rule tightened controls on blackout lights for ECCN 0A606 items or USML Category VII items by moving such blackout lights from proposed ECCNs 0A606.y to 0A606.x.

13.3.4. Final Changes Regarding Surface Vessels of War, Submersible Vessels and Oceanographic Equipment. The second set of BIS and DDTC final rules, issued on July 8, 2013, also finalized the changes to USML Categories VI, covering surface vessels of war, and Category XX, covering submersible vessels and oceanographic equipment. 78 *Fed. Reg.* 40922 (July 8, 2013); 78 *Fed. Reg.* 40892 (July 8, 2013).

13.3.4.1. Summary of Final DDTC Rules on USML Categories VI and XX. With respect to Category VI, for surface vessels of war and special naval equipment, the rule will narrow the types of vessels controlled on the USML and remove the rest to the CCL. For example, it will remove harbor entrance detection devices, currently controlled in Category VI(d) to the CCL. Additionally, Category VI(d) will no longer include any submarines, which will be moved to Category XX to join the rest of the "submersible vessels" currently controlled on the USML. Most importantly, the rule will remove from Category VI all or almost all generic parts, components, accessories and attachments specially designed for Category VI items. Instead, with respect to parts, components, accessories, and attachments, the revised Category VI will include only certain specific enumerated types of parts, components, accessories and attachments. The rule also will revise ITAR § 121.15, which currently lists particular types of ships and equipment that are included in Category VI, to provide greater clarity.

Essentially, the new Category VI will be a relatively simple category, as follows:

(a) Subcategory (a) will cover warships, and combatant vessels (and would refer the reader to ITAR § 121.15 for a specific listing);
(b) Subcategory (b) will control other vessels not identified in paragraph (a) (and would again refer the reader to ITAR § 121.15);
(c) Subcategory (c) will control developmental vessels and specially designed parts/components, etc., therefor developed under a contract with the U.S. Department of Defense;
(d) Subcategory (d) will be empty and reserved;
(e) Subcategory (e) will cover naval nuclear propulsion plants and prototypes, and special facilities for their construction, support and maintenance;
(f) Subcategory (f) will control a long list of specific parts/components, etc. that will remain controlled in Category VI; and
(g) Subcategory (g) will control technical data related to foregoing.

Other than the parts and components of developmental vessels that will be covered in subcategory (c), and the specific parts and components that would be enumerated in subcategory (f), *all* parts and components, accessories and attachments will be moved to the CCL.

With respect to Category XX, the final rule again explained that any submarines currently classified in Category VI will be moved to Category XX, so that all submersible vessels will be consolidated into one USML category. Additionally, any naval nuclear propulsion power plants for submersible vessels now controlled in Category VI will move to Category XX. As with Category VI, Category XX will also refer the reader to a separate ITAR section, ITAR § 121.14, which will more clearly define and identify the "submersible vessels and related articles" included in the category. However, unlike Category VI, the final Category XX will still include *all* specially designed parts, components, accessories and attachments, as opposed to covering only a short list of specifically enumerated items. Thus, the final Category XX will look like this:

- Subcategory (a) will control submersible and semi-submersible vessels, listing some and also referring the reader to ITAR § 121.14 for further detail;
- Subcategory Paragraph (b) will cover engines, certain electric motors, and naval nuclear propulsion plants and their land prototypes, and special facilities for their construction, support, and maintenance;
- Subcategory (c) will cover all specially designed parts, components, accessories and attachments, and associated equipment, including production, testing, and inspection equipment and tooling; and
- Subcategory (d) will cover technical data for the foregoing.

Of all of the USML categories that have been addressed in proposed or final rules so far, Category XX is probably the one that looks the most like the current version. This is because the government determined in reviewing Category XX that submarines and related equipment, for the most part, provide the United States with a critical military and intelligence advantage, and many of the technologies are available only in the United States. Thus, with the exception of a few submersible vessels and related items detailed below, there will not be much movement to the CCL. Nonetheless, the revised Category XX will provide a more positive list of controlled items than does the current Category XX, which is an improvement.

13.3.4.2. Summary of Final BIS Rule on Surface Vessels of War, Submersible Vessels and Oceanographic Equipment. The final BIS rule will create a total of nine new 600 Series ECCNs. ECCNs 8A609, 8B609, 8C609, 8D609 and 8E609 will be the new homes for vessels of war and related items removed from USML Category VI, and ECCNs 8A620, 8B620, 8D620 and 8E620 will house the submersible vessels and related items removed from USML Category XX. Note that there will be no ECCN 8C620, because there were no "materials" for submersible vessels that will be removed from the USML to the CCL. The final rule will also place in 8A620 most items from the Wassenaar Munitions List related to submersible vessels and currently classified under ECCN 8A018.

 bflowe@bcr-dc.com

Regarding the new ECCNs related to vessels of war, ECCN 8A609.a will cover any vessel of war not specified in the USML, and a note to ECCN 8A609.a will enumerate several specific vessels that will be covered, including, for example, non-submersible submarine rescue ships and unarmed amphibious warfare craft. ECCN 8A609.b will cover certain non-magnetic diesel engines. Paragraphs .c through .w will be reserved for the identification of additional items in the future, and paragraph .x will cover parts/components, etc., specially designed for the commodities "enumerated in 8A609 (except for 8A609.y) or a defense article enumerated in USML Category VI and not specified elsewhere on the USML or in 8A609.y." Paragraph .y will specify certain enumerated parts/components, etc., subject to AT-1 only controls. ECCN 8B609 will be for test, inspection, and production equipment, ECCN 8C609 for materials, ECCN 8D609 for software and ECCN 8E609 for technology.

The new ECCNs related to submersible vessels will be set up very similarly, except that there will be no ECCN 8C620 for materials, and ECCN 8A620 will include certain items from the Wassenaar Munitions List that are now classified in ECCN 8A018, as noted above. Another significant difference will be that paragraph .x will cover only parts, components, etc. "that are specially designed for a commodity enumerated in ECCN 8A620 (except for 8A620.b or 8A620.y" and will not cover any parts/components, etc. for items in USML Category XX. This is because, unlike with the revised Category VI, which will include only specific enumerated parts and components, all specially designed parts and components for submersible vessels and related equipment will remain in the revised Category XX (not just those that are specifically enumerated).

13.3.5. Final Changes Regarding Materials and Miscellaneous Items. The DDTC and BIS final rules of July 8, 2013 also covered changes to be made to USML Category XIII, to remove some items and more specifically list the remaining items, and to change the name of the category from "Auxiliary Military Equipment" to "Materials and Miscellaneous Articles." 78 *Fed. Reg.* 40922 (July 8, 2013); 78 *Fed. Reg.* 40892 (July 8, 2013).

13.3.5.1. Summary of Final DDTC Rule on USML Category XIII. The DDTC final rule will remove from Category XIII the entirety of subcategory (c), currently covering self-contained diving and underwater breathing apparatus. Subcategory (c) will be reserved for later use. The items currently in subcategory (c) will move to ECCN 8A620.f.

Subcategory (b), covering military information security systems, such as military cryptographic and cryptanalytic systems, is largely unchanged, but some of the wording will be tweaked a bit. This subcategory was already described in a relatively high degree of specificity.

The remaining subcategories, covering such items as certain ablative materials, armor, energy conversion devices, and tooling and equipment, are greatly revamped, resulting in a much less all-inclusive, and more positive listing of specific items meeting specific technical parameters. Accordingly, although the new category will comprise a lot more text, it actually includes fewer items.

 bflowe@bcr-dc.com

13.3.5.2. Summary of Final BIS Rule on Materials and Miscellaneous Items. The items removed from USML Category XIII will be housed in new ECCNs 0A617, 0B617, 0C617, 0D617 and 0E617. The final rule will also move to the new ECCN 0A617.y construction equipment built to military specifications and currently classified under ECCN 0A918, containers specially designed for military use, military field generators, and military power-controlled searchlights and related items. ECCN 0A617 will also include the following items when specially designed for military applications and when not enumerated in the USML or in another 600 Series ECCN:

- Concealment and deception equipment, and specially designed parts, components, accessories and attachments;
- Ferries, bridges, and pontoons;
- Test models specially designed for the development of defense articles controlled by USML Categories IV, VI, VII and VIII;
- Metal embrittlement agents.

Unlike with some of the other new ECCNs, ECCN 0A617 will not include a catch-all control in paragraph x. for all parts and components specially designed for the items listed because USML Category XIII does not include such a catch-all control. If a part, component, accessory or attachment is intended to be controlled, it will be specified in the ECCN paragraph where the end-item is listed.

Consistent with the classification convention in the CCL, ECCN 0B617 will control test, inspection and production equipment for the items in ECCN 0A617, and ECCN 0D617 and ECCN 0E617 will control software and technology for such items, respectively. ECCN 0C617 will control materials, coatings and treatments for signature suppression specially designed for military use to reduce detectability or observability and not controlled elsewhere in USML Category XIII or ECCNs 1C001 or 1C101.

13.3.6. Proposed Changes Regarding Energetic Materials. On May 2, 2012, DDTC issued a proposed rule to revise USML Category VII by making it more of a positive list and removing certain items from the USML. 77 *Fed. Reg.* 25944 (May 2, 2012). Also on May 2, 2012, BIS issued a proposed rule to describe how the items removed from USML Category V would be controlled under the EAR, among other things. 77 *Fed. Reg.* 25932 (May 2, 2012).

13.3.6.1. Summary of Proposed DDTC Rule on USML Category V. The following are some of the main changes in the proposed rule:

- Broad catch-all language in (a)(35), (b)(7), (c)(10), (e)(19), and (f)(21) would be removed. Some items now caught by such catch-all language would be specifically listed in Category V.
- Limited catch-all language would be added to or retained in (a)(37), (a)(38), (b)(1), (b)(2), (b)(3), (c)(3), (c)(4), and (f)(4)(xv). The proposed catch-all in (a)(38) is a revised form of the catch-all currently in (a)(32), with the main revision being a change in the detonation velocity parameter from 8700 meters per

 bflowe@bcr-dc.com

second to 8000 meters per second to match the criteria from the Nuclear Suppliers Group.

- The interpretation now in (i)(3) concerning mixtures/compounds would be significantly revised. Category V(i)(3) now states: "The resulting product of the combination of any controlled or non-controlled substances compounded or mixed with any item controlled by this subchapter is also subject to the controls of this category." This interpretation would be moved to (i)(2) and the first sentence of (i)(2) would state: "The resulting product of the combination or conversion of any substance controlled by this category into an item not controlled will no longer be controlled by this category provided the controlled item cannot easily be recovered through dissolution, melting, sieving, etc."
- The movement of certain classified items from USML Category XVII (Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated) to Category V(h).

13.3.6.2. Summary of Proposed BIS Rule on Energetic Materials. Under its proposed rule, BIS would create four new ECCNs (i.e., 1B608, 1C608, 1D608 and 1E608) to control materials removed from USML Category V. BIS would also amend ECCN 1C111 to control some of the aluminum powder and hydrazine and derivatives thereof that would be removed from USML Category V. As part of BIS's effort to consolidate into one series of ECCNs EAR-controlled Wassenaar Munitions List items and former USML items, the proposed rule would move equipment for the production of explosives and solid propellants from ECCN 1B018.a to new ECCN 1B608. Related software would be moved from ECCN 1D018 to new ECCN 1D018. The proposed rule would move commercial charges and devices containing energetic materials from ECCN 1C018 to new ECCN 1C608, except for chlorine trifluoride, which is not on the Wassenaar Munitions List and would be transferred from ECCN 1C238 to ECCN 1C111.a.3.f. ECCN 1C238 would be removed.

13.3.7. Proposed Changes Regarding Protective Equipment and Shelters. On June 7, 2012, DDTC and BIS issued their back-to-back rules to address USML Category X, covering personal protective equipment and shelters. 77 *Fed. Reg.* 33688 and 77 *Fed. Reg.* 33698 (June 7, 2012).

13.3.7.1. Summary of Proposed DDTC Rule on USML Category X. DDTC did a great job in the proposed rule making Category X a much more positive list of controlled items, citing specific parameters for control. In its current form the Category covers all protective personnel equipment and protective shelters designed for military applications, regardless of whether they are specifically enumerated or not. Moreover, those items that are enumerated are not described with much specificity. For example, the category currently includes "body armor," a fairly broad term. In contrast, the only body armor the proposed rule would include would be body armor "providing a protection level equal to or greater than NIJ Type IV." All other body armor would be moved to the CCL.

Other items that would remain in Category X are the following (we list them all because there are so few):

 bflowe@bcr-dc.com

- Personal protective clothing, equipment or face paints specially designed to protect against or reduce detection by radar, IR, or other sensors at wavelengths greater than 900 nm;

- Integrated helmets incorporating optical sights or slewing devices, which include the ability to aim, launch, track or manage munitions;

- Helmets and helmet shells providing a protection level equal to or greater than NIJ Type IV;

- Goggles, spectacles, or visors, employing other than common broadband absorptive dyes and UV inhibitors as a means of protection, with optical density greater than 3 that protect against (i) thermal flashes associated with nuclear detonations or (ii) certain specified wavelengths; and

- Developmental personal protective equipment and shelters, and specially designed parts, components, accessories and attachments therefor, developed under contract with the Defense Department.

These are the only end-items covered. Any other end-items currently included in Category X would be moved to the CCL.

Regarding parts, the proposed USML Category X would cover only ceramic or composite plates that provide protection equal to or greater than NIJ Type IV, lenses for the goggles, spectacles and visors that are controlled in Category X as end-items, and any parts, components, accessories or other equipment that is classified, contain classified software, or are manufactured or developed with classified information. All other specially designed parts would be moved to the CCL.

13.3.7.2. Summary of Proposed BIS Rule on Protective Equipment and Shelters. The BIS proposed rule would create four new ECCNs for the items removed from USML Category X, ECCNs 1A613, 1B613, 1D613 and 1E613. There would be no 1C613 as no specific materials would be controlled here. The proposed rule would also move military helmets currently listed under ECCN 0A018 to the new ECCN 1A613, and would amend ECCN 1A005, where certain body armor is currently classified.

ECCN 1A613.a would control armored plate specially designed for military use but not included on the USML; ECCN 1A613.b would control shelters specially designed to provide ballistic protection or protect against nuclear, biological, or chemical contamination; ECCN 1A613.c would control military helmets with protection less than NIJ level IV; ECCN 1A613.d would control certain specific soft body armor and protective garments; ECCN 1A613.e would control other personal protective equipment, such as handheld ballistic shields specially designed for military use. Paragraphs .f through .w would be reserved for future use, and paragraph .x would control parts, components, accessories and attachments specially designed for any of the foregoing items. Additionally, conventional military steel helmets (currently classified under ECCN 0A988) would be covered under paragraph y.1. Anti-gravity suits, pressure suits, and

 bflowe@bcr-dc.com

atmosphere diving suits currently controlled in USML Category X would all move to ECCN 9A610.

The other new ECCNs, 1B613, 1D613 and 1E613, would cover test, inspection, and production equipment, software and technology, respectively, for the items in ECCN 1A613.

13.3.8. Proposed Changes Regarding Military Training Equipment. In the last of a very busy May and June for proposed rules, DDTC and BIS published their parallel proposals regarding the removal of certain military training equipment from the USML to the CCL on June 13, 2012. The DDTC proposed rule slated a number of less sensitive articles of training equipment for removal from the USML (77 *Fed. Reg.* 35317 (June 13, 2012)), and the BIS proposed rule (77 *Fed. Reg.* 35310 (June 13, 2012)), as with the previous proposals, created new ECCNs where these items would be housed and specifically described.

13.3.8.1. Summary of Proposed DDTC Rule on USML Category IX. The first thing the proposed DDTC rule would change about Category IX is its title. Right now it covers "Military Training Equipment and Training." The proposed new title would be changed to "Military Training Equipment" to make clear that only actual training equipment itself, and no training, is covered. As explained in the Preamble to the proposed rule, "training on a defense article would be a defense service covered under the category in which the defense article is enumerated." Thus, training foreign persons in use of firearms would be a defense service classified in the firearms category of the USML (Category I), not as "training" under Category IX. This is intuitive and makes sense, and the change to the title should remove any ambiguity that exists as the USML is currently written.

The next major change is the significantly more "positive" listing in subcategory (a) of the training equipment that would remain controlled in USML Category IX, as opposed to the broad and quite vague description that exists now. The revised subcategory (b) would, similarly, provide a much more positive list of specific simulation devices controlled (a vast improvement from the existing subcategory) (b), which simply states "Simulation devices for the items covered by this subchapter." The proposed rule also notes that a couple of items that could be thought of as "simulators" – i.e., radar target and infrared scene generators – will be classified in USML Categories XI(a) and XII(c), respectively.

Perhaps most important of the proposed changes, *all* tooling and production equipment, currently controlled in subcategory (c), and *all* generic parts, components, accessories and attachments, currently controlled in subcategory (d), "that are in any way specifically designed or modified for a defense article, regardless of their significance to maintaining a military advantage for the United States," will be moved to the CCL. Subcategory (c) through (f) of Category IX in its current form would cease to exist. Subcategory (e) would control a smaller universe of technical data and defense services.

The proposed rule also explained that parts and components, etc., of a simulator that are the same as the parts and components for the actual end-item being simulated will be classified in

the category of the end-item. While this is not necessarily a change, it is useful that the proposed rule makes this clear in case there is ever any doubt.

13.3.8.2. Summary of Proposed BIS Rule on Military Training Equipment. The BIS proposed rule explained that the military training items no longer warranting control on the USML would be relocated to four new ECCNs in Category 0 of the CCL: ECCNs 0A614, 0B614, 0D614 and 0E614. Because the new classifications are so short, we will excerpt them here for your reference. The proposed ECCN 0A614 would cover:

> a. "Equipment,specially designed" for military training that is not enumerated in USML Category IX. **Note**: This entry includes operational flight trainers, radar target trainers, flight simulators for aircraft classified under ECCN 9A610.a, human-rated centrifuges, radar trainers for radars classified under ECCN 3A611, instrument flight trainers for military aircraft, navigation trainers for military items, target equipment, armament trainers, military pilotless aircraft trainers, mobile training units and training "equipment" for ground military operations.
> b. [reserved] . . .
> w. [reserved]
> x. "Parts," "components," and "accessories and attachments" that are ''specially designed'' for a commodity controlled by this entry or an article enumerated in USML Category IX, and not specified elsewhere in the CCL or the USML. **Note:** Forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by material composition, geometry, or function as commodities controlled by ECCN 0A614.x are controlled by ECCN 0A614.x.

77 Fed. Reg. 35310, 35316. ECCNs 0B614, 0D614 and 0E614 are essentially derivative of 0A614 (and USML Category IX in the case of ECCN 0B614) (i.e., ECCN 0B614 would cover test, inspection, and other production equipment specially designed for the production of ECCN 0A614 or Category IX items; ECCN 0D614 would cover software specially designed for the development, production, operation or maintenance of ECCNs 0A614 or 0B614 items; and ECCN 0E614 would cover technology required for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of ECCN 0A614, 0B614 or 0D614 items.

Unlike end items in other 600 Series ECCNs, according to BIS's proposed rule, end items classified in ECCNs 0A614 and 0B614 would be eligible for License Exception STA without prior approval by BIS. Parts and components in 0A614 and 0B614 would also be eligible for STA without prior approval by BIS. Further, these two ECCNs would be eligible for License Exceptions LVS (limited value shipments) up to $1500, TMP (temporary exports), and RPL (servicing and parts replacement).

13.3.9. Proposed Changes Regarding Military Electronics. On July 25, 2013,

DDTC issued a proposed rule to revise USML Category XI on military electronics. 78 *Fed. Reg.* 45018 (July 25, 2013). Also on July 25, 2013, BIS issued a proposed rule to describe how the items removed from USML Category XI would be controlled under the EAR. 78 *Fed. Reg.* 45026 (July 25, 2013). These were the second set of proposed rules to revise USML Category XI and move certain military electronics items to the CCL. DDTC and BIS both published earlier proposed rules on military electronics items, in November 2012, but received so many comments they decided to issues revised proposals and solicit further public feedback.

13.3.9.1. Summary of Proposed DDTC Rule on USML Category XI.
The DDTC proposed rule would amend current subcategories (a)(1), (a)(3)-(5) to more specifically enumerate the items controlled therein. Subcategory (a)(6), controlling military computers, would be moved to the CCL. Subcategory (a)(7) would cover developmental electronic equipment or systems funded by the Defense Department. However, a note to (a)(7) expressly states that it would not cover items that are i) in production, ii) subject to the EAR pursuant to a Commodity Jurisdiction determination, or iii) identified in the relevant Defense Department contract as being developed for both civil and military applications. Subcategories (a)(8)-(12) would be added to cover a number of new specific items, such as unattended ground sensors, and electronic sensor systems for concealed weapons, among other things, meeting certain parameters.

Subcategory (b), currently covering a vague laundry list of items ("electronic system or equipment for search, reconnaissance, collection, monitoring, direction finding, display, analysis, or production of information from the electromagnetic spectrum and electronic systems or equipment that counteracts electronic surveillance), would only be reworded a bit and would thus still be a broad subcategory, but would also provide an illustrative list of specific systems that are fairly objectively described.

Most importantly, Category XI would no longer generally cover all specially designed parts and components, but would only control those specifically enumerated in a new subcategory (c). Recall that the existing Category XI already expressly excluded specially designed parts and components that were "in normal commercial use," but that was so vague as to almost be meaningless. The proposed specifically described list of covered parts and components will be a welcome change.

13.3.9.2. Summary of Proposed BIS Rule on Military Electronics.
The corresponding BIS proposed rule for military electronics would house the items to be removed from USML Category XI and certain cryogenic and superconductive equipment designed for installation in military vehicles and that can operate while in motion, currently classified under USML Categories VI, VII, VIII and XV. Military electronics and related items would be covered in four new ECCNs in CCL Category 3: 3A611, 3B611, 3D611 and 3E611. The cryogenic and superconducting equipment would be controlled in four new ECCNs in CCL Category 9: 9A620, 9B620, 9D620 and 9E620. A few other ECCNs and EAR provisions would be amended to make some conforming changes.

 bflowe@bcr-dc.com

Notably, this proposed rule would cover certain military computers, telecommunications equipment, and radar specially designed for military use, under the new 600 Series ECCNs in CCL Category 3 rather than creating new ECCNs in CCL Categories 4 (computers), 5 (telecommunications), and 6 (radar), as might be expected. However, BIS will add cross-references in those other CCL categories to prevent confusion. Specifically, there will be a new ECCN 4A611, the heading of which states "Computers, and parts, components, accessories, and attachments 'specially designed' therefor, 'specially designed' for military use that are not enumerated in any USML category are controlled by ECCN 3A611;" and a new ECCN 5A611, the heading of which states "Telecommunications equipment, and parts, components, accessories, and attachments 'specially designed' therefor, 'specially designed' for military use that are not enumerated in any USML category are controlled by 3A611."

ECCN 3A611.a would be a "catch-all" control of sorts, covering all "electronic equipment, end items and systems specially designed for military use that are not enumerated in either a USML category or another 600 Series ECCN." 3A611 would also cover certain specified microwave monolithic integrated circuits (MMIC) power amplifiers, discrete microwave transistors, high frequency surface wave radar, and microelectronic devices. Paragraph .y would slate a number of items to AT only controls, including electric couplings, connectors, fans, and heat sinks, among many others. ECCNs 3B611, 3D611 and 3E611 would cover certain related test, inspection, and production equipment, software and technology.

The new 600 Series ECCNs in CCL Category 9 would control the items described above, and would include no paragraph .y parts and components subject only to AT controls.

13.3.10. Proposed Changes Regarding Missiles. On January 31, 2013, DDTC and BIS published parallel proposals regarding the removal of certain items from USML Category IV, covering launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs and mines. 78 *Fed. Reg.* 6765 (Jan. 31, 2013) and 78 *Fed. Reg.* 6750 (Jan. 31, 2013). The DDTC proposed rule would also change a number of ITAR sections addressing the Missile Technology Control Regime ("MTCR") Annex, to provide a new method of identifying articles common to the MTCR Annex and the USML. Currently, items in the MTCR Annex are listed both in ITAR § 121.16 and in the USML. The rule would remove ITAR § 121.16 and instead would identify the MTCR Annex items by placing the parenthetical "(MT)" at the end of each USML section containing Annex items.

13.3.10.1. Summary of Proposed DDTC Rule on USML Category IV. The DDTC proposed rule would result in a much, much more "positive" list of controlled items, with much more detailed descriptions of objective control criteria and parameters. As with other proposed rules, this would result in a much longer USML Category IV (since controlled items are more specifically enumerated), but one that actually covers less.

Among other things, the proposed rule would remove ITAR controls over demolition blocks, blasting caps, and military explosive excavating devices. Also, ablative materials, though they will remain under ITAR control, would be moved to USML Category XIII(d).

 bflowe@bcr-dc.com

13.3.10.2. Summary of Proposed BIS Rule on Missiles. The BIS proposed rule would create eight new 600 Series ECCNs, four each in Categories 0 and 9 of the CCL, and make conforming amendments to a few existing Categories 0 and 9 ECCNs. The demolition blocks, blasting caps and explosive excavating devices discussed in the preceding section would be moved to the new ECCN 0A604. There would be no paragraph .y in this new ECCN. ECCNs 0B604 would control test, inspection and production equipment for the items in 0A604, and 0D604 and 0E604 would control certain related software and technology respectively. There would be no 0C604 for materials.

A new ECCN 9A604 would control thermal batteries specially designed for USML Category IV systems. It would also control certain enumerated parts and components, such as components for ramjet, scramjet, pulse jet or combined cycle engines controlled under USML Category IV, and also all other specially designed parts, components, accessories and attachments for 9A604 items and for defense articles controlled under USML Category IV and not otherwise specified on the USML or CCL. The entire ECCN, like other 600 Series ECCNs, would be subject to NS-1 and RS-1 controls, but certain items would also be subject to Missile Technology (MT-1) controls. None of the 9X604 ECCNs would include paragraph .y items subject only to AT controls. ECCNS 9B604, 9D604 and 9E604, cover certain related test, inspection, and production equipment, software and technology equipment, respectively.

13.3.11. Proposed Changes Regarding Nuclear Items. On January 13, 2013, DDTC issued a proposed rule to amend USML Category XVI, covering nuclear weapons and related articles. 78 *Fed. Reg.* 6269 (Jan. 13, 2013). There was no corresponding BIS rule. This is because, as explained in the Preamble to the proposed rule, export of most of the items currently classified in USML Category XVI are under the control of the Department of Energy ("DoE") pursuant to the Atomic Energy Act and the Nuclear Non-Proliferation Act. Accordingly, once finalized, the rule would remove any such items subject to DoE control from USML Category XVI. The only items that would remain in Category XVI would be modeling or simulation tools that model or simulate the environments generated by nuclear detonations of the effects of these environments on systems, subsystems, components, structures, or humans, and related technical data and defense services. That's it. Category XVI would thus be the shortest of all USML categories that actually list items (i.e., excluding USML Category XVIII for classified items, and Category XXI for miscellaneous items). Additionally, nuclear radiation detection and measurement devices currently controlled in subcategory (c) would become subject to the EAR, but these items are already classified in existing ECCN 1A004.c.2 or 2A291.e, so, again, no corresponding BIS rule was needed.

13.3.12. Proposed Changes Regarding Spacecraft and Satellites. On January 2, 2013, President Obama signed the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) ("2013 NDAA"). Section 1261 of the 2013 NDAA amended Section 1513 of the Strom Thurmond National Defense Authorization Act of Fiscal Year 1999 (Pub. L. 105-261) ("1999 NDAA") by returning to the President the authority to determine which regulations should govern the export of spacecraft, satellites and related articles. Between 1999 and 2013, legislation conferred jurisdiction over such items to the State Department under the ITAR. Section 1248 of the 2013 NDAA required the Secretaries of Defense and State carry out an

assessment of the risks associated with removing satellites and related components from the USML. The Departments of State and Defense published their findings and recommendations in a report provided to Congress in April 2012 (the "1248 Report").

On May 24, 2013, DDTC and BIS published parallel proposals for removing certain satellites and related items from the USML to the CCL. The DDTC proposed rule (*78 Fed. Reg. 31444*) (May 24, 2013) describes more precisely the specific spacecraft and related articles that continue to warrant control under the USML. The DDTC proposed rule also provides a new definition of "defense service." The BIS proposed rule (*78 Fed. Reg. 31431*) (May 24, 2013) creates a new "500 Series" of ECCNs to control spacecraft systems and associated equipment that would be removed from Category XV. The proposed rules are based largely on the recommendations made by the Departments of State and Defense in the 1248 Report.

The greatest impact on industry will likely be reduced administrative costs and reduced delay for exports of items that will be moved from the USML to the CCL. By transferring certain articles from Category XV to the CCL, industry may be able to reduce its burden by taking advantage of the elimination of certain licensing requirements (e.g. *de minimis* reexports), greater availability of License Exceptions, simplification of application procedures, and reduction (or elimination) of DDTC registration fees.

13.3.12.1. Summary of Proposed DDTC Rule on USML Category XV. The proposed rule makes several changes to USML Category XV. Paragraphs (a) and (e) remove the current broadly-worded controls and catch-all provisions, and more specifically describe the articles that will continue to be controlled by the ITAR. Commercial satellites and related equipment are to be transferred to the CCL. Those items remaining on the USML include spacecraft, satellites, and manned or unmanned space vehicles, that: (1) are designed to mitigate effects of, or detect, nuclear detonations; (2) track ground, airborne, missile or space objects using imaging, infrared, radar or laser systems; (3) conduct signals or measurement and signatures intelligence; (4) provide space-based logistics, assembly or servicing of spacecraft; (5) are anti-satellite or anti-spacecraft; (6) have space-to-ground weapons systems; or (7) have specified electro-optical remote sensing capabilities or characteristics. Proposed paragraph (e) contains a list of the specific types of spacecraft parts, components, accessories, attachments, equipment, or systems that will remain ITAR-controlled. Spacecraft that are not identified in paragraph (a), and parts, components, accessories, and attachments specially designed for spacecraft but not specifically enumerated in paragraph (e) will be transferred to the CCL.

Paragraph (c) of the proposed rule will continue, for the time being, to control certain Global Positioning System ("GPS") receiving equipment. However, once Category XII is revised and implemented, DDTC intends to move the GPS items controlled under paragraph (c) to Category XII. The radiation-hardened microelectronic circuits that are currently covered under paragraph (d) will be shifted under the proposed rule to the CCL and will be controlled by the new ECCN 9A515.d.

The proposed rule also includes a second revised definition of "defense service." On April 13, 2011, the State Department published a proposed revision of the definition of defense

service, with the intention of narrowing the definition to exclude certain forms of assistance or services that do not warrant ITAR control. Thirty-nine parties submitted comments recommending changes to the April 13, 2011 definition. Rather than proceed to a final rule on the definition, the State Department republished the revised definition on May 24, 2013 as another proposed rule and is seeking further comment.

Although a thorough discussion of the definition is out of the scope of the memorandum, the proposed rule revises the definition of defense service by more clearly describing what constitutes a defense service and what does not. Paragraphs (a)(1) through (a)(5) include a specific list of activities that would be considered defense services, including the furnishing of assistance in the integration of a satellite or spacecraft to a launch vehicle or in a launch failure analysis. On the other hand, paragraphs (b)(1) through (b)(5) contain a non-exhaustive list of the type of activities that would not constitute defense services in the future (e.g., providing basic-level maintenance to defense articles). DDTC is accepting comments on the proposed definition of defense service until July 8, 2013.

13.3.12.2. Summary of Proposed BIS Rule on Spacecraft and Satellites.

Unlike other items that are being transferred from the USML to the CCL, commercial satellites and associated equipment are not munitions, and therefore are not being controlled under the new 600 Series. Instead, the BIS proposed rule creates a new "500 Series" of ECCNs specifically to control Category XV items moved to the CCL. These items will be controlled by new ECCNs 9A515, 9B515, 9D515 and 9E515 (collectively, "9X515"). All items controlled by 9X515 ECCNs would be subject to National Security (NS Column 1) and Regional Stability (RS Column 1), as well as Antiterrorism (AT Column 1) controls. Some of the items would also be subject to Missile Technology (MT) controls in certain cases. Licensing policy for the 500 Series items will proceed on a case-by-case review. However, applications for 500 Series items destined to countries subject to U.S. arms embargo (Country Group D:5) will be reviewed consistent with U.S. arms embargo policies (presumptive denial). Additionally, applications for 500 Series items destined to China, North Korea, or any country that is state sponsor or terrorism, will be subject to a policy of denial.

Most 500 Series items will be eligible for several License Exceptions, including STA (Strategic Trade Agreement), LVS (Limited Value Shipments) up to $1500, TMP (temporary exports), GOV (U.S. Government), and RPL (servicing and replacement parts). The use of License Exception STA for 500 Series items would require the consignee to consent to an end-user check by the U.S. Government in addition to standard consignee statement required for all STA transactions. However, the 600 Series-specific STA requirements will not be applicable to the 500 Series items.

The proposed rule adopts the same *de minimis* thresholds (and direct-product rule) for the 500 Series as proposed for the 600 Series items. Foreign-made items that incorporate any amount of U.S.-origin 500 Series items would be subject to the EAR when destined to a country that is subject to a U.S. arms embargo. However, a foreign-made item that incorporates U.S.-origin 500 Series items destined to a country that is not subject to a U.S. arms embargo would be eligible for *de minimis* treatment, and would not be subject to the EAR if the value of its U.S.-origin controlled content does not exceed 25% of the foreign-made item's value. This will be

 bflowe@bcr-dc.com

extremely beneficial to U.S. satellite component manufacturers, as foreign manufacturers will have less incentive to avoid U.S.-origin parts and components in order to avoid being subject to U.S. export control laws.

13.3.13. Final Rule Establishing New Temporary Holding 0Y521 Series ECCNs, Analogous to USML Category XXI for Miscellaneous Items. In a final rule issued April 13, 2012, BIS amended the CCL and made conforming changes to other parts of the EAR to create the new 0Y521 series ECCNs, a temporary holding category for items that warrant control on the CCL but are not yet identified in an existing ECCN. 77 *Fed. Reg.* 22191 (Apr. 13, 2012). Items are to be added to the new 0Y521 series ECCNs when BIS, in agreement with DDTC and the Defense Department, identifies an item that should be controlled because it provides a significant military or intelligence advantage, or otherwise justifies control for foreign policy reasons. The new ECCN 0Y521 series will thus create a more nimble and transparent mechanism for identifying and controlling items in the short-term that may be of concern to the U.S. Government, such as emerging technologies. It should also facilitate the movement of some items from the USML to the CCL. In the past, the jurisdictional transfer of some items has been delayed and even blocked because such items would have fallen all the way to EAR99. DDTC and BIS had previously agreed to move certain items only after new ECCNs with RS controls had been established.

The new 0Y521 series will also serve as a CCL analogue to the USML's Category XXI, covering miscellaneous items. However, unlike USML Category XXI, classification of items under ECCN 0Y521 is intended to be only of limited duration. Also, no items will be moved from USML Category XXI, because Category XXI does not actually enumerate any specific items. Indeed, it covers "any article *not specifically enumerated* in other categories of the [USML] which has substantial military applicability and which has been specifically designed, developed, configured, adapted, or modified for military purposes [and technical data and defense services directly related to the same.]" USML Category XXI (emphasis added).

As explained in the Preamble to the proposed rule, once an item is designated under ECCN 0Y521, one of three things will happen next. The U.S. Government will: (i) work to adopt a permanent control for the item in cooperation with the relevant multilateral export control regime; (ii) determine some other appropriate longer-term control over the item; or (iii) determine that the item does not warrant control on the CCL, in which case the item will revert to EAR99 status.

Items classified under ECCN 0Y521 will remain classified there for one year following the date of the publication of the final rule classifying them, unless they are reclassified under a different ECCN before the end of the year, or BIS issues a new rule affirmatively extending the ECCN 0Y521 classification. Ordinarily, BIS may only extend an ECCN 0Y521 classification for two one-year periods, up to a total of three years. This period of time was believed to provide sufficient time for BIS to seek multilateral agreement on the item's classification elsewhere in the CCL. However, a further extension will be permitted if the Under Secretary for Industry and Security determines such extension is required to protect U.S. national security or foreign policy interests. Unfortunately, this means that the ECCN 0Y521 classifications could effectively be

permanent. Moreover, such classifications are exempt from the EAR Part 756 appeals process. Hopefully, extension beyond three years will be very rare in practice. That is certainly BIS's stated intention and expectation.

Any items classified in the new ECCNs will be subject to RS-1 controls, requiring a license for export to all destinations except Canada. Initially, License Exception GOV will be the only license exception available, and only if an item is for official use by personnel and agencies of the U.S. Government. However, BIS noted that it may authorize use of additional license exceptions in the future, on an item-specific basis, with the concurrence of DDTC and the Defense Department.

The new ECCN 0Y521 series is comprised of five separate ECCNs: 0A521, 0B521, 0C521, 0D521 and 0E521. However, the items classified under the new 0Y521 series ECCNs will not actually appear with the rest of the CCL in Supplement No. 1 to Part 774. Although the ECCN headings will appear in CCL Category 0, the ECCNs will direct the reader to a new Supplement No. 5 to Part 774 for the actual listing of the items covered. As BIS explained in the Preamble to the final rule, this unique structure will allow items to be added to the new 0Y521 series ECCNs that would otherwise be more appropriately classified in CCL categories other than Category 0, without having to add new XY521 series ECCNs to all ten categories of the CCL (which would amount to a total of 50 new ECCNs total). The table format of Supplement No. 5 also provides for easier identification of the information relevant to the exporter (e.g., date of initial classification, date of expiration, etc.), than the current structure of ECCNs in Supplement No. 1 to Part 774.

Given the breadth and scope of the CCL and USML, BIS anticipates that items will be classified under 0Y521 sparingly. Indeed, after almost a year, only one rule has been issued classifying items under 0Y521, certain biosensor systems, software and technology. 78 *Fed. Reg.* 18814 (Mar. 28, 2013). Nonetheless, having the new ECCNs in place and available going forward will facilitate the continuous process of reviewing and updating the CCL, and provide a mechanism for quickly addressing emerging technologies.

13.4. What to Expect Next.

The Administration moved with all deliberate speed to achieve as much as possible before President Obama's first term ended, and has continued to make methodical progress since the second term began. Reforming the USML so that it controls only items truly warranting control as defense items and also to make the USML more objective are the reforms that should have the most far-reaching and positive impact from both a national security and economic standpoint, so it makes sense that the Administration has pursued these goals so aggressively. While legislative action will be required for full implementation of a Single Control List, if the Administration is able to finalize all of the proposed changes to the USML and CCL so far, great progress will have been made even if the lists remain separate. Indeed, the migration of so many minor parts and components and other items from the USML to the CCL will amount to the biggest change to U.S. export controls in over a decade, even if nothing further is achieved. The biggest winners will be companies who make and export low-level parts and components for

defense articles because many or most such parts and components moved to the CCL and the vast majority of such transferred parts and components will be exportable under License Exception STA's terms and limitations. However, some may vuew that the benefits of the jurisdictional transfers are outweighed by the complexity of having to deal with both DDTC and BIS controls on projects that previously were governed exclusively or almost entirely by DDTC controls.

Proposed rules have been issued addressing the USML categories that will probably see the most changes, and we expect to see more categories addressed (in proposals) and some more finalized by the end of the year. The Administration is still aiming to have the process completed by the end of 2013, although this seems very ambitious.

Slow progress toward more harmonized enforcement and adoption of a single IT platform and single license application form will also continue and will hopefully reach fruition. The Single Licensing Agency should prove to be the heaviest lift as it would be such a fundamental reform of the current system, requiring a number of entrenched stakeholders to relinquish some of their control and influence.

13.5. Interim Final Rule Amending ITAR Brokering Regulations.

On December 19, 2011, DDTC published a proposed rule (76 *Fed. Reg.* 78578) modifying the provisions of the ITAR relating to "Brokering" and "Brokering Activities." The December 19, 2011 proposed rule was widely viewed by industry as a drastic expansion of the scope of the brokering regulations, as it sought to extend control over all foreign persons located outside the United States who engaged in brokering activities on behalf of a U.S. person. More than thirty parties filed comments with DDTC recommending changes to the proposed rule. Rather than issuing a final rule, DDTC made significant additional changes based on the public comments and issued a new interim final rule on August 26, 2013 titled "Amendment to the International Traffic in Arms Regulations: Registration and Licensing of Brokers, Brokering Activities, and Related Provisions. 78 *Fed. Reg.* 52680 (the " Interim Rule"). The Interim Rule will become effective on October 25, 2013. DDTC will accept comments on the Interim Rule through October 10, 2013, and will publish a final rule thereafter notifying of any changes to the Interim Rule pursuant to public comment assessment.

The Interim Rule is a drastic improvement over the December 19, 2011 proposed rule, although some in industry remain unhappy that the scope of the Interim Rule is more expansive than the current brokering regulations contained in Part 129 of the ITAR. Although an exhaustive discussion of the Interim Rule is outside the scope of this memorandum, below is a summary of some of the key amendments:

- **Revised Definition of "Broker".** The Interim Rule limits the scope of who constitutes a "Broker" to any person who engages in the business of "Brokering Activities", and who is also: (a) A U.S. person wherever located, or (b) a foreign person located in the U.S., or (c) a foreign person located outside the U.S. where the foreign person is owned or controlled by a U.S. person. (*emphasis added*). *See* §129.2(a). The terms "owned" and "controlled" are defined by a note to §129.2(a). To the dismay of many in industry, the

 bflowe@bcr-dc.com

Interim Rule removes from the current definition the requirement that the person "acts as an agent for others" in "return for a fee, commission, or other consideration." A person may now engage in Brokering Activities, even if it does so without compensation or other consideration.

- **Revised Definition of "Brokering Activities".** The Interim Rule also drastically revises the current definition of "Brokering Activities." The Interim Rule defines Brokering Activities as "any action on behalf of another to facilitate the manufacture, export, permanent import, transfer, reexport, or retransfer of a U.S. or foreign defense article or defense service, regardless of its origin." *See* §129.2(b). Section 129.2(b) provides a non-exhaustive list of the types of activities that would constitute Brokering Activities, including: financing, insuring, transporting, freight forwarding, soliciting, promoting, negotiation, contracting for, arranging or otherwise assisting in the purchase, sale, transfer, loan or lease of a defense article or defense service. Unlike the current regulations, the Interim Rule clarifies the types of activities that do not fall within the definition.

- **Actions on behalf of Affiliates**. One important amendment included in the Interim Rule is the clarification that "activities performed by an affiliate… on behalf of another affiliate" do not constitute Brokering Activities. *See* §129.2(b)(2). The Interim Rule inserts a new definition of an "Affiliate" into the ITAR. Section 120.44 states that: "An affiliate of a registrant is a person that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, such registrant." A note to §120.40 defines "control" as having the authority or ability to establish or direct the general policies or day-to-day operations of the firm, and presumes "control" exists where there is ownership of 25 percent or more of the outstanding voting securities, so long as no other person controls an equal or larger percentage. Although this clarification is appreciated by industry, it is unclear how DDTC intends to regulate the actions of registrants on behalf of their affiliates. Because the definition of Affiliate does not include a "registrant", a literal reading of the Interim Rule suggests that actions by a registrant on behalf of its affiliate could be considered by DDTC as constituting Brokering Activities. It remains to be seen whether any comments will be submitted to DDTC regarding this issue, or whether DDTC will amend this loophole in the final rule.

- **Prior Approval of Brokering Activities.** Rather than requiring prior approval for Brokering Activities related to all USML items, as the December 19, 2011 proposed rule required, the Interim Rule specifies those USML items that require prior approval, and those items that do not. *See* §§129.4 and 129.5. The Interim Rule also specifies which activities are exempt for prior approval. One major exemption included in the Interim Rule is for those persons whose business is exclusively financing, insuring, transporting, or freight forwarding. *See* §129.3(b)(2).

 bflowe@bcr-dc.com

- **Consolidated Registration.** The Interim Rule makes a few significant changes to Broker registration requirements. Currently, a registrant is required to file one DS-2032 Statement of Registration ("Registration Statement") to cover its manufacturer/exporter activities, and a separate Registration Statement to cover its Brokering Activities, along with two separate fees. The Interim Rule authorizes the consolidation of the two Registration Statements into one, and eliminates the requirement for submitting a second fee. *See* §129.3(d). The Interim Rule also authorizes registrants to include their U.S. or foreign subsidiaries and other affiliates (under certain circumstances specified in §129.8(a)) on their Registration Statements. Note 2 to §129.8(d) clarifies that changes to the Registration Statement to combine an existing broker registration with an existing manufacturer/exporter registration should be provided as part of the annual registration renewal, rather than upon the effective date of the Interim Rule.

Amendments to Annual Brokering Report. Currently, Annual Brokering Reports are due by the end of the calendar year. The revised regulations provide that Annual Brokering Reports shall be submitted as an attachment to the registrants' annual registration renewal. *See* §129.10(a). Section 129.10(b) mandates that additional information be included in the Annual Brokering Reports beyond that which is currently required, including, for example, information about the identity, nationality, address, and role of all individuals who participated in the Brokering Activities.

13.6. Embargo and Sanctions Developments.

13.6.1. New Developments in Sanctions Against Iran.

It seems lately that Congress and the Obama Administration have been in a race to impose additional sanctions on Iran. This includes enhancing existing sanctions, imposing new sanctions, and talking about future sanctions.

Perhaps the most interesting news in this area occurred in early October 2011, when an Iranian-American was indicted for the attempted assassination of Saudi Arabia's ambassador to the United States and bombing of the Israeli embassy. This, among other things, resulted in the July 2012 enactment of the Iran Sanctions, Accountability and Human Rights Act of 2012, which for the first time will prohibit foreign subsidiaries of U.S. companies from doing business with Iran. Discussed further below, this is a major development in the sanctions against Iran and will have far-reaching consequences. Also in October, the Treasury Department gained a new tool with a final rule implementing Section 104(e) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"). CISADA Section 104(e) requires U.S. banks to report to the Financial Crimes Enforcement Network ("FinCen") information about transactions of their foreign correspondent banks that might indicate CISADA violations. This

 bflowe@bcr-dc.com

led to the famous statement by a high level Treasury official that: "You have a choice to make. You can continue to do business with us or you can continue to do business with designated banks, but you can't do both."

13.6.1.1. Iran Sanctions, Accountability and Human Rights Act of 2012. On July 31, 2012, Congress passed the Iran Threat Reduction and Syria Human Rights Act of 2012 ("ITRSHRA"). It had originally been introduced in early 2011, but stalled for over a year in the Senate. An amended version passed the House almost unanimously and the Senate by voice vote. President Obama signed it into law on Friday, August 10, 2012.

Most important, the ITRSHRA requires the President, within 60 days of the signing of the law (i.e., by October 9, 2012), to apply the same restrictions on all trade transactions with Iran that apply to a "U.S. person" to any non-U.S. person organization that is "owned or controlled" by a "U.S. person."

(b) *Prohibition*. – Not later than 60 days after the date of the enactment of this Act, the President shall prohibit an entity owned or controlled by a United States person and established or maintained outside the United States from knowingly engaging in any transaction directly or indirectly with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited by an order or regulation issued pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) if the transaction were engaged in by a United States person or in the United States.

This is essentially the same standard applied in the Cuban Assets Control Regulations ("CACR").

The ITRSHRA defines "own or control" as follows:

(2) OWN OR CONTROL.—The term "own or control" means, with respect to an entity—
(A) to hold more than 50 percent of the equity interest by vote or value in the entity;
(B) to hold a majority of seats on the board of directors of the entity; or
(C) to otherwise control the actions, policies, or personnel decisions of the entity.

The first two provide objective standards for ownership or control, however, the third prong is more subjective but may be sufficient to render further transactions with Iran illegally, based on the participation of a U.S. affiliate in the management of foreign affiliates, and/or the presence of U.S. persons in upper management positions at either the

 bflowe@bcr-dc.com

non-U.S. parent or non-U.S. operating companies.

The Iranian Transactions Regulations ("ITR") define a "U.S. person" to include not just U.S. business organizations, but also U.S. citizens, permanent residents wherever located and regardless of who their employer is, as well as any individual person physically located in the United States. So, "control" of a non-U.S. person by U.S. person individuals would fall within the scope of the act.

Prior to this law, individual U.S. person involvement in transactions with Iran by entities organized under other countries' laws was already prohibited by the ITR, but those prohibitions could be overcome by a lack of direct or indirect involvement of U.S. person employees in the transaction, or by recusal of the U.S. persons involved. Thus, U.S. *in personam* jurisdiction was triggered by the involvement of the individual in the particular transactions with Iran, and could be eliminated by the removal of such persons from involvement. (Separate *in rem* jurisdiction could and can apply based on U.S.-origin items reexported to Iran in that form or after incorporation into non-U.S.-origin items.)

However, under the new law, jurisdiction over the non-U.S. entity is triggered if the participation of a U.S. affiliate or activities of U.S. person individuals in the management of the non-U.S. entity is sufficient to "otherwise control the actions, policies, or personnel decisions of the [non-U.S.] entity."

13.6.1.1.1. <u>Context Yet to be Defined</u>. It remains to be seen whether OFAC will further define this term in the context of the ITR. It has not done so in the context of Cuba. OFAC has not provided any written guidance regarding the interpretation of what degree of "control" is required to render a non-U.S. subsidiary a "U.S. person" for CACR purposes.

Our consultations with former OFAC officials, including the former Director, General Counsel, and members of the Counsel's staff, indicated that OFAC has traditionally looked at the issue on a case-by-case basis for CACR purposes, and has not set any bright line rules, other than a presumption of control where a U.S. person has more than a 50% ownership interest in a foreign company (reflected explicitly in paragraph (a) of the ITRSHRA definition), or a lower, but nonetheless controlling percentage, where no other party held a greater interest. None of the former officials could recall an OFAC CACR enforcement case where ownership interests were outside the United States but management control was exercised from the United States.

Practitioners in the sanctions field, based on experience with OFAC enforcement approaches and informal discussions with OFAC officials over the years, believe that OFAC

 bflowe@bcr-dc.com

would likely determine that control is established clearly when a foreign affiliate is wholly-owned by U.S. persons; is controlled by U.S. persons in terms of its day-to-day operations; or U.S. person senior managers or directors have control over major corporate decisions.

The concept of derivative applicability of sanctions based on ownership or control appears in the OFAC regulations elsewhere with respect to targets of sanctions. Numerous OFAC programs target sanctions against Specially Designated Nationals ("SDNs"). All such programs include language that extends the designation to cover entities that are "owned" by the SDN. Some OFAC programs, such as the Sudanese Sanctions Regulations, also have language in the designation criteria for SDNs that apply sanctions to entities that are "owned or controlled" by the target government or an already-designated SDN.

OFAC has issued written guidance interpreting what degree of ownership would trigger derivative SDN status on the basis of ownership by the SDN, applying the same presumptions discussed above. The guidance mentions that some of the programs also impose derivative SDN status based on "control," but does not provide further criteria to determine when the indicia of control are sufficient to trigger derivative SDN status.

Thus, the OFAC guidance would not be of much assistance, so we will have to consider other sources to determine whether those organizations would become U.S. persons for CACR purposes due to their control by individuals who are U.S. persons.

13.6.1.1.2. Potential Guidance from Other U.S. Trade Regulations Regarding the Interpretation of "Controlled." Many experienced practitioners in the field recommend (in the singular ABA National Institute Programs on Economic Sanctions and others) looking to similar regulatory language in the U.S. Commerce Department's Antiboycott Regulations, EAR Part 760 (the "Antiboycott Regulations"), for examples of what constitutes "controlled in fact" affiliates. While these regulations are based on a different statutory authority and issued by a different U.S. government agency, they may be instructive in gauging the likely scope of OFAC's interpretation of "owned or controlled."

We also note as a threshold matter that jurisdiction under the Antiboycott Regulations is limited to "controlled-in-fact" affiliates of "domestic concerns," defined to include only partnerships, companies, corporations, associations, or other business entities. The CACR's definition applies not only to entities that are "owned or controlled" by U.S. incorporated entities, but also by U.S. person individuals. Accordingly, the examples provided in the Antiboycott Regulations are focused on indicators of corporate ownership or control, but still may be instructive.

 bflowe@bcr-dc.com

Another significant distinction is that, unlike the CACR, the Antiboycott Regulations do not define a "U.S. person" to include an individual who is not a U.S. citizen or resident, but who is physically present in the United States (unless he or she is acting on behalf of a U.S. domestic concern). Accordingly, the Antiboycott Regulations, unlike the CACR, would not contemplate jurisdiction based on activities of a foreign concern's senior manager who is not a U.S. citizen or resident, but who is located in the United States.

The Commerce Antiboycott Regulations provide:

> (1) [...] "Control in fact" consists of the authority or ability of a domestic concern to establish the general policies or to control day-to-day operations of its foreign subsidiary, partnership, affiliate, branch, office, or other permanent foreign establishment.
>
> (2) A foreign subsidiary or affiliate of a domestic concern will be presumed to be controlled in fact by that domestic concern, subject to rebuttal by competent evidence, when:
>
> (i) The domestic concern beneficially owns or controls (whether directly or indirectly) more than 50 percent of the outstanding voting securities of the foreign subsidiary or affiliate;
>
> (ii) The domestic concern beneficially owns or controls (whether directly or indirectly) 25 percent or more of the voting securities of the foreign subsidiary or affiliate, if no other person owns or controls (whether directly or indirectly) an equal or larger percentage;
>
> (iii) The foreign subsidiary or affiliate is operated by the domestic concern pursuant to the provisions of an exclusive management contract;
>
> (iv) A majority of the members of the board of directors of the foreign subsidiary or affiliate are also members of the comparable governing body of the domestic concern;
>
> (v) The domestic concern has authority to appoint the majority of the members of the board of directors of the foreign subsidiary or affiliate; or
>
> (vi) The domestic concern has authority to appoint the chief operating officer of the foreign subsidiary or affiliate.

EAR § 760.1(c)(1)-(2).

We have consulted in the past on this issue with officials from the Office of Antiboycott

 bflowe@bcr-dc.com

Compliance, including current members of the legal staff and the former Director. They acknowledged that enforcement of such a case would likely be difficult under the Antiboycott Regulations due to the limitation of jurisdiction to "controlled-in-fact" subsidiaries of domestic corporate entities (as opposed to companies that are "controlled-in-fact" by a U.S. person individual). We know of no enforcement cases other than in the ownership context. However, they believed that the exercise of direct control over day-to-day operations or general policies of a non-U.S. company by an individual who held concurrent positions with a U.S. company could reasonably be analogous to a U.S. domestic concern exercising "control-in-fact" of a foreign affiliate under an "exclusive management contract".

OFAC officials have stated in the past that the term "control" under the CACR does apply to cases other than ownership, but have not articulated what the relevant standard might be. Many experts believe they would apply principles similar to those articulated by the EAR Antiboycott Regulations. We do not have sufficient information to know how those indicators would apply but commend them to your review.

Our understanding is that it would be an unprecedented action for OFAC to apply the "control" test to treat subsidiaries of a non-U.S.-organized company as "U.S. persons" based on control by lower- level U.S. managers when there is no U.S. legal ownership of the subsidiaries or top-level management involved, however it is difficult to predict how OFAC will act in response to a new statutory authority and clear direction. There is very little sympathy these days for doing business with Iran.

13.6.1.1.3. Potential Interpretation of Control under ITRSHRA. Combining these concepts with the ITRSHRA definition, which expands the definition of "control" to include the capacity to "control the actions, policies, or personnel decisions" of a non-U.S. entity, it seems reasonable to conclude that the presence of a U.S. person individual in top-level management positions of a non-U.S. entity, such as chief executive officer, chief operating officer, chief financial officer, or president quite likely triggers the ITRSHRA prohibition.

Further, if the U.S. affiliate or personnel working for that affiliate are responsible for the establishment of day-to-day operating policies of a non-U.S. entity, it would likely trigger the prohibition.

It is less clear whether U.S. persons acting as lower-level executives (e.g., vice president and below) would, by itself, be sufficient to trigger the prohibition. We would be surprised if OFAC provides any granular advice regarding the level at which U.S. person participation would not trigger the prohibition.

 bflowe@bcr-dc.com

We note that it has been at least the informal policy of some companies to treat all foreign affiliates as "owned or controlled" for CACR purposes, if even out of an abundance of caution. The vast majority of enforcement actions or sanctions are settlements, and few companies seem to wish to challenge the matters in court, where the administration is accorded substantial deference in applying foreign policies. It may be difficult to justify reaching a different conclusion with respect to Iran, since the CACR and ITRSHRA provisions are very similar, with the ITRSHRA provisions arguably providing more specific illustration of what constitutes control by a U.S. person.

13.6.1.1.4. Wind Down and Divestment Provision. The ITRSHRA requires the President to take action within 60 days of the enactment of the law. Right on schedule on October 9, 2012, President Obama issued Executive Order No. 13628 implementing certain sanctions set forth in the ITRSHRA., Section 4(a) of the Executive Order confirmed the extension of the Iranian sanctions to entities owned or controlled by a U.S. Person and established or maintained outside the United States which knowingly engage in any transaction, directly or indirectly, with the Government of Iran or any person subject to the jurisdiction of the Government of Iran, if the transaction were engaged in U.S. Person or in the United States.

If an owned or controlled foreign affiliate ceases its business with Iran prior to October 9, 2012 neither the foreign affiliate nor the U.S. owning/controlling person will be liable.

The ITRSHRA contains a limited "safe harbor" clause, which eliminates derivative liability for an owning/controlling U.S. company for the actions of its owned or controlled foreign affiliate. This clause is effective only if the U.S. entity either divests itself of ownership in the foreign affiliate (where jurisdiction is triggered by ownership) or where the U.S. person ceases to control the foreign affiliate (where jurisdiction is triggered by control).

> (d) *Applicability*. – Subsection (c) [derivative liability for the U.S. parent] shall not apply with respect to a transaction described in subsection (b) by an entity owned or controlled by a United States person and established or maintained outside the United States if the United States person divests or terminates its business with the entity [meaning its owned or controlled foreign subsidiary] not later than the date that is 180 days after the date of the enactment of this Act.

Reading all the sections together, there is thus up to a 60-day period for both the foreign entity and the U.S. parent/controlling entity to stop the Iran business or divest/withdraw from control. Then, if the business continues after that, the foreign entity would be in violation, and

 bflowe@bcr-dc.com

the U.S. entity is also derivatively liable unless it divests or otherwise terminates its business with the foreign entity within 180 days of the enactment of ITRSHRA. Note that the divestment/cessation of U.S. control would also terminate any violation by the foreign firm, because the basis of jurisdiction is ownership or control by a U.S. person. However, any foreign affiliate transactions that take place between the amendment of the ITR and divestment/cessation of control would still be susceptible to prosecution.

From a practical enforcement perspective, OFAC is perhaps also less likely to prosecute a case against foreign firms that take good-faith actions to wind down business within a reasonable time, since 60 days is a very short time to do so. However, OFAC is also more likely to afford such consideration to firms that make voluntary disclosures if they are not able to cease the business fully within 60 days or divest/cease control within 180 days. (OFAC has licensed companies that ceased doing business in Iran to take certain limited actions (paying taxes, etc.) involved in winding down such business.)

13.6.1.1.5. AG/MED Exemptions and Licensing. It is not clear the extent to which existing licensing policies will apply to the activities of owned or controlled foreign affiliates involving Iran, but a plain reading of the applicable statutes suggests that they should.

The Trade Sanctions Reform and Export Enhancement Act of 2000 ("TSRA") terminated, or required licenses for, any U.S. unilateral agricultural and medical sanctions issued pursuant to the International Emergency Economic Powers Act ("IEEPA") or Trading with the Enemy Act ("TWEA"). This led to the institution of general licenses and specific licensing procedures by OFAC and BIS for exports of qualifying agricultural and medical products to Cuba, Iran, and Sudan. ISAHRA directs the President to amend IEEPA-based sanctions against Iran, so the TSRA should also limit the applicability of the expanded ISAHRA sanctions to qualifying activities by owned or controlled foreign affiliates. So, the existing general licenses authorizing the negotiation of executory contracts related to the sale of licensable items, contingent on obtaining U.S. licenses, should extend to the TSRA-eligible activities of owned or controlled foreign affiliates.

Some sections of ISAHRA seem to acknowledge that the TSRA policy should remain, but not all sections. Complications apply when there is no U.S. *in rem* jurisdiction over the Ag/Med item (less than 10% U.S.-origin content), and OFAC has said on occasion that it has no authority to license non-U.S. transactions in the context of the CACR, but we have been able to obtain TSRA licenses for foreign-made items for sale to Iran, and once for sale to Cuba. OFAC's position on Cuba may be affected by provisions of the Cuban Democracy Act of 1992, which arguably requires a more conservative licensing policy as to transaction involving sales by

 bflowe@bcr-dc.com

foreign subsidiaries of non-U.S.-origin items. That said, the extension of *in personam* jurisdiction by ITRSHRA may also affect OFAC's interpretation of the scope of its authority to issue licenses pursuant to TSRA. Based on past experience, we also anticipate that OFAC will not necessarily be speedy in resolving these sorts of complicated legal issues.

As a practical matter, we note that the existing TSRA licensing program is a very slow process. OFAC recently issued a report on TSRA licensing activities from October 2008 through September 2010. In that report, OFAC indicated that there had been a 54% increase in license applications, and that the average processing time of such applications was approximately 90 business days (over 4 calendar months) to issue a license. At the time of the report, OFAC had a backlog of over 200 cases. Our experience with processing times from September 2010 to the present has been that they have remained at least as slow, if not slower.

So, even if a company were to decide today to submit license applications for eligible activities, it is highly likely that there will be an interruption of business, because it is unlikely that OFAC will issue licenses within a 60-day timeframe. The likelihood of receiving a license quickly will likely be further diminished by an anticipated uptick in TSRA license applications by owned or controlled foreign affiliates and the need for OFAC counsel to interpret application of TSRA to the new law.

It should also be noted that TSRA licenses are also subject to significant restrictions with respect to which Iranian financial institutions can be involved in the payment for goods. All Iranian financial institutions, even the Iranian Central Bank and private Iranian banks, have been designated as Government of Iran SDNs, and all of the Government of Iran-owned banks are additionally designated as SDNs under Global Terrorism and Weapons of Mass Destructions Sanctions programs. Coupled with recent extremely large fines against non-U.S. banks for their participation in Iranian transactions, it has become very difficult, as a practical matter, to make payment arrangements for licensed or exempt transactions involving Iran. A group of companies sought clarifying language in the statute to encourage U.S. bank financing of TSRA transactions, but we cannot find such language in ITRSHRA itself. Hopefully, subsequently issued House or Senate Reports will provide some clarification.

13.6.1.1.6. <u>New Requirements for Disclosure to the Securities and Exchange Commission.</u> Section 219 of the Act also took the novel approach of amending the Securities and Exchange Act of 1934 to include a requirement for listed companies to disclose certain activities relating to Iran. The amendment to the Securities Act requires any company trading on U.S. exchanges to disclose certain activities of it or its affiliates which "knowingly engaged in" conduct that involves specific provisions of the Iran Sanctions Act or CISADA, or "knowingly conducted any transaction or dealing" with persons the property of

 bflowe@bcr-dc.com

which is blocked under several Executive Orders. These activities include dealings in Iran's energy sector, development of weapons of mass destruction, dealings with the Islamic Revolutionary Guard Corps, and dealings with persons whose property and interests in property are blocked pursuant to enumerated Executive Orders (Executive Orders 13224 and 13382).

The information that is required to be disclosed includes a detailed description of each such activity, including: (1) the nature and extent of the activity; (2) the gross revenues and net profits, if any, attributable to the activity; and (3) whether the company or its affiliate(s) intend to continue the activity. Disclosure to the Securities and Exchange Commission ("SEC") is required in regular reports which are due 180 days after the legislation is enacted, which would take the requirement to February 9, 2013. Upon receiving the disclosure, the SEC is then required to transmit a report to (1) the President; (2) the Committees on Foreign Affairs and on Financial Services of the House of Representatives; and (3) the Committees on Foreign Relations and on Banking, Housing, and Urban Affairs of the Senate; and to make the information available to the public by posting it on the Internet site of the SEC. Finally, the Act requires the President to investigate the activity disclosed to the SEC and determine whether sanctions should be imposed.

The difficult aspect of this disclosure requirement will be in determining the "knowingly" standard which prompts the disclosure requirement.

13.6.1.2. Clamping Down Hard on Iran's Petroleum and Petrochemical Sectors. On November 21, 2011, the President issued Executive Order 13590, expanding the reach of the Iran Sanctions Act and CISADA. 76 *Fed. Reg.* 72609 (Nov. 23, 2011). This Executive Order authorized the Secretary of State to impose sanctions on persons determined to have provided certain goods, services, technology, or support that contributes to either Iran's development of petroleum resources or to Iran's production of petrochemicals. Specifically, this expansion of CISADA authorizes sanctions on persons who knowingly: 1) sell, lease, or otherwise provide to Iran, goods, services, technology or support that could directly and significantly contribute to the enhancement of Iran's ability to develop petroleum resources located in Iran, if a single transaction has a fair market value of $1 million or more, or a series of transactions from the same entity have a fair market value of $5 million or more in a twelve-month period; and 2) sell, lease, or otherwise provide to Iran, goods, services, technology, or support that could directly and significantly contribute to the maintenance or expansion of its domestic production of petrochemical products, if a single transaction has a fair market value of $250,000 or more, or if a series of transactions by the same entity has a fair market value of $1 million or more in a twelve-month period. This extraterritorial reach expanded the sanctions to include prohibitions on: foreign exchange transactions; banking transactions; property transactions in the United States; U.S. Export-Import Bank financing; U.S. export licenses;

 bflowe@bcr-dc.com

imports into the United States; loans of more than $10 million from U.S. financial institutions; U.S. Government procurement contracts; and, for financial institutions, designation as a primary dealer or repository of U.S. Government funds.

13.6.1.3. Treasury Designates Iran as Primary Money Laundering Concern. Also, in its most aggressive action against the Iranian banking sector to date, the Treasury Department, under Section 311 of the USA PATRIOT Act, identified the entire Iranian banking sector, including the Central Bank of Iran, as a primary money laundering concern. In taking this action, the Treasury Department stated that it would impose rules to require U.S. financial institutions to: 1) terminate correspondent accounts with Iranian banks, including the Central Bank of Iran, and any non-Iranian bank that is 50% or more owned by two or more Iranian banks; 2) apply "special due diligence" to their correspondent accounts "to guard against their improper indirect use by Iranian banking institutions;" 3) take a "risk-based approach in deciding what, if any, other due diligence measures they should adopt to guard against the improper direct use of their correspondent accounts by Iranian banking institutions"; and 4) take "all appropriate steps" to prevent a correspondent account from being used by a foreign bank "to provide indirect access to an Iranian banking institution."

13.6.1.4. Blocking of All Iranian Banks. In February of 2012, President Obama, by Executive Order 13599, ordered the blocking of all property or interests in property of the Government of Iran, including the Central Bank of Iran, and all Iranian financial institutions, and all persons determined by the Secretary of the Treasury to be owned or controlled by or acting for or on behalf of any of those parties when the property comes within the United States or within the possession or control of U.S. persons. 77 *Fed. Reg.* 6659 (Feb. 8, 2012).

The big change here is that transactions involving the Government of Iran or Iranian financial institutions that previously were only required to be rejected now must be blocked. OFAC did simultaneously issue two General Licenses. General License A authorizes transactions under existing general licenses set forth in the Iran Transactions Regulations ("ITR"), or under existing OFAC specific licenses, including Trade Sanctions Reform and Export Enhancement Act ("TSRA") licenses among others. This provides some relief, as it would enable a U.S. person holding a license under the TSRA to receive payment from an Iranian customer originating from an Iranian bank, provided that the funds transit through a third-country bank (U.S. banks cannot conduct business with Iranian banks) and the Iranian bank is not an SDN. General License B authorizes U.S. depository institutions and registered brokers and dealers in securities to process noncommercial, personal remittances, to or from Iran, or for or on behalf of individuals ordinarily resident in Iran, as long as these individuals are not blocked or are not included within the meaning of the Government of Iran.

 bflowe@bcr-dc.com

13.6.1.5. New Definition for Owned or Controlled. Also in March 2012, OFAC amended Section 560.313 of the ITR to redefine when an entity is owned or controlled by the Government of Iran. 77 *Fed. Reg.* 16170 (Mar. 20, 2012). Under the old definition, an entity was considered to be owned or controlled by the Government of Iran if the latter owned a "majority or controlling interest" in the entity, or the entity was otherwise controlled by the Iranian Government. Under the new definition, an entity is treated as being owned or controlled by the Government of Iran if the latter owns a "50 percent or greater interest," or a controlling interest in the entity, or the entity is otherwise controlled by the Iranian Government. The new rule means that an entity in which the Iranian Government has only a 50 percent (but not a majority) interest is treated as part of the Government of Iran, regardless of whether the Government, in fact, controls the entity. This new definition, renders the general rule of "know your customer" that much more important.

13.6.1.6. OFAC Issues Interpretive Guidance on Scope of Software General License. On March 20, 2012, OFAC issued interpretive guidance on the scope of the personal communications general license issued in March of 2010 (75 *Fed. Reg.* 10997 (Mar. 10, 2010), codified at ITR § 560.540), which authorizes the exportation of certain services and software incident to the exchange of personal communications over the Internet. *See* Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran (Mar. 20, 2012), *at* http://www.treasury.gov/resource-center/sanctions/Programs/Documents/internet_freedom.pdf. The interpretive guidance is designed to ensure that the sanctions on Iran do not have an "unintended chilling effect" on the ability of companies to provide personal communications tools to individuals in Iran.

According to the guidance, illustrative services and software which fall within the scope of Section 560.540 of the ITR include: 1) personal communications software (e.g. Yahoo Messenger, Google Talk, Microsoft Live, Skype (non-fee based)); 2) updates to personal communications software; 3) personal data storage (e.g. Dropbox); 4) browsers/updates (e.g. Google Chrome, Firefox, Internet Explorer); 5) plug-ins (e.g. Flashplayer, Shockwave, Java); 6) document readers (e.g. Acrobat Readers); 7) free mobile applications related to personal communications; and 8) feed readers and aggregators (e.g. Google Feed Burner).

The guidance also announced a favorable licensing policy for requests to export to Iran services and software not within the scope of the General License at ITR § 560.540 but that nonetheless directly benefit the Iranian people. Accordingly, OFAC will issue specific licenses on a case-by-case basis for the exportation of other, including fee-based, services and software incident to sharing information over the Internet, provided the software is classified as EAR99, is not subject to the EAR, or is classified by BIS as mass market software under ECCN 5D992 of the EAR. OFAC specifically stated that this Statement of Licensing Policy applies to services

 bflowe@bcr-dc.com

and software such as web hosting, online advertising, fee-based mobile apps, and fee-based Internet communications services.

13.6.1.7. General License Authorizes Export of Food to Iran and Sudan. The tension between the ever-tightening sanctions on Iran on the one hand, and the need to comply with existing U.S. law allowing the export of food to Iran on the other hand, was relieved somewhat when OFAC issued a General License replacing the one-year specific license requirement for exports of most food to Iran. 76 *Fed. Reg.* 63191 (Oct. 12, 2011). The General License (also applicable to Sudan) authorizes the exportation and reexportation of "food" to the Government of Iran, to any individual or entity in Iran, or to persons in third countries purchasing specifically for resale to such persons or entities in Iran. For purposes of the General License, "food" is defined as:

> Items that are intended to be consumed by and provide nutrition to humans or animals in Iran, including vitamins, minerals, food additives and supplements, and bottled drinking water, and seeds that germinate into items that are intended to be consumed by and provide nutrition to humans or animals in Iran.
>
> 31 C.F. R. § 560.530(a)(2)(ii).

The General License also authorizes related transactions, including the making of shipping arrangements, obtaining insurance, arranging financing and payment, receipt of payment, and entry into contracts, so long as all exports and reexports are shipped within the twelve-month period beginning on the date of the signing of the contract for export or reexport. The export and reexport of items not covered by the definition of food, but covered by the TSRA authority, such as non-food agricultural items, medicine, medical devices, are still subject to the one-year license requirement. The General License does not authorize exports or reexports to military, law enforcement (which are still subject to the one-year license requirement) or to blocked persons, and therefore exporters must continue to screen for sanctioned customers, even if the item for export or reexport is otherwise covered by the authority of the General License.

13.6.1.8. OFAC Issues Iran General License D, Authorizing Certain Transactions Incident to Personal Communications. On May 30, 2013, OFAC issued Iranian General License D authorizing the exportation or reexportation of certain services, software, and hardware incident to personal communications from the United States or by U.S. persons to persons in Iran. Excepting transactions that are otherwise exempt from the Iranian Transactions and Sanctions Regulations (31 CFR Part 560), General License D permits the exportation or reexportation from the United States or by U.S. persons (wherever located), including by entities

 bflowe@bcr-dc.com

owned or controlled by a U.S. person and established or maintained outside the United States (subject to the conditions set forth in 31 C.F.R. §560.556), to persons in Iran of the following:

- Fee-based services for the exchange of personal communications via the internet (such as instant messaging, chat and email, social networking, photo and video sharing, web browsing, and blogging);
- Fee-based software subject to the EAR that is necessary for the foregoing, so long as such software is designated as EAR99 or classified under ECCN 5D992.c;
- Certain software and hardware specified in the general license, including without limitation certain mobile and satellite telephones, modems, routers, and WiFi access points, residential satellite receiver terminals, personal computing devices, antivirus and antitracking software, VPNs, SSLs, and all software necessary for the operation thereof; and
- Consumer-grade Internet connectivity services, and the provision, sale, or leasing of capacity on telecommunications transmission facilities (such as satellite or terrestrial network connectivity) incident to personal communications.

General License D does not permit any of the following:

- The exportation or reexportation, directly or indirectly, of the services, software, or hardware specified above with knowledge or reason to know that such services, software, or hardware are intended for the Government of Iran;
- The exportation or reexportation, directly or indirectly, of the services, software, and hardware specified above to any person whose property and interests in property are blocked pursuant to any part of 31 C.F.R. chapter V;
- The exportation or reexportation, directly or indirectly, of commercial-grade Internet connectivity services or telecommunications transmission facilities (such as dedicated satellite links or dedicated lines that include quality of service guarantees); or
- The exportation or reexportation, directly or indirectly, of web-hosting services that are for purposes other than personal communications (e.g., web-hosting services for commercial endeavors) or of domain name registration services.

General License D also authorizes U.S. depository institutions and U.S. registered brokers or dealers in securities to transfer funds from Iran or for the benefit of a person in Iran in furtherance of an underlying transaction otherwise authorized by the general license, so long as such transfers are consistent with 31 C.F.R. § 560.51.

13.6.1.9. <u>OFAC Issues Iran General Licenses E and F, Authorizing Certain Transactions Related to Humanitarian Activities or Athletic Exchanges</u>. On September 10, 2013, OFAC issued two general licenses that authorize certain humanitarian-related activities by nongovernmental organizations in Iran and athletic exchanges involving Iran and the United States.

 bflowe@bcr-dc.com

Subject to certain restrictions and reporting requirements as detailed in the general license, General License E authorizes the exportation or reexportation of services and funds transfers (up to US$500,000 within a 12-month period) by nongovernmental organizations ("NGOs") in support of certain not-for-profit humanitarian activities designed to benefit the people of Iran.

General License E authorizes NGOs to export or reexport services to Iran for activities related to humanitarian projects to meet basic human needs, such as the provision of donated health-related services; operation of orphanages; provision of relief services related to natural disasters; distribution of donated articles, such as food, clothing, and medicine, intended to be used to relieve human suffering; and donated training related to any of the foregoing.

General License E also authorizes NGOs to export or reexport services or transfer funds in support of non-commercial reconstruction projects in response to natural disasters (for a period of up to two years following the disaster), for environmental and wildlife conservation projects involving endangered species of fauna and flora and their supporting habitats, and for human rights and democracy building projects, such as the sponsorship of and attendance and training at conferences in Iran related to human rights projects, democracy building, or civil society development; efforts to increase access to information and freedom of expression; and public advocacy, public policy advice, polling, or surveys relating to human rights and democracy building.

General License F authorizes the importation and exportation of certain services in support of professional and amateur sporting activities and exchanges involving the United States and Iran. The importation of Iranian-origin services into the United States or other dealing in such services, and the exportation or reexportation of services, directly or indirectly, from the United States or by a United States person related to professional and amateur sporting activities and exchanges involving the United States and Iran are authorized, including, but not limited to, activities related to exhibition matches and events, the sponsorship of players, coaching, refereeing, and training.

General License F does not authorize the exportation or reexportation of the above-specified services to any person whose property and interests in property are blocked pursuant to any part of 31 C.F.R. chapter V other than part 560.

13.6.2. New Sanctions Against Foreign Persons Who Evade the Iran or Syria Sanctions. The 2012 sanctions season started off with Executive Order 13608, which suspended entry into the United States of foreign sanctions evaders with respect to both Iran and Syria. 77 *Fed. Reg.* 26409 (May 3, 2012). This Executive Order applies to any foreign person who violates, attempts to violate, conspires to violate, or causes a violation of any license order, regulation, or prohibition of U.S. sanctions against Iran or Syria, or has facilitated deceptive transactions for or on behalf of any person subject to U.S. sanctions concerning Iran or Syria.

It is not clear exactly who this additional sanction is directed toward as it only seems to be directed at individuals who have violated already existing sanctions, but this will presumably

 bflowe@bcr-dc.com

give OFAC additional ammunition to go after foreign persons traditionally thought to be beyond OFAC jurisdiction. The Executive Order also applies to entities that are owned or controlled by any person who violates, attempts to violate, or conspires to violate existing sanctions, or facilitates deceptive transactions.

The additional sanction provided by this Executive Order is that OFAC may prohibit all transactions, dealings, whether direct or indirect, involving such foreign person, including exporting, reexporting, importing, selling, purchasing, transporting, swapping, brokering, approving, financing, facilitating, or guaranteeing in or related to any goods, services or technology in or intended for the United States or provided by or to U.S. persons.

13.6.3. New Sanctions on Those Who Facilitate Certain Human Rights Abuses By Iranian or Syrian Governments. Combining the desire for more and stricter sanctions against Iran with outrage over human rights abuses and military action by Syria against its own people, on April 22, 2012, President Obama signed Executive Order 13606. 77 *Fed. Reg.* 24571 (Apr. 24, 2012). This Executive Order targets individuals or entities facilitating computer or network disruption, monitoring, or tracking, to facilitate or commit serious human rights abuses against the people of Iran and Syria.

Using the acronym "GHRAVITY" (which stands for "Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology") this Executive Order blocks all property and interests in property of specified individuals or entities determined to have operated or directed the operation of information and communications technology that facilitates computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Governments of Iran or Syria, that is in the United States or that comes within the possession or control of any U.S. person, including any foreign branch. The restrictions of the Executive Order extend to anyone who has sold, leased, or otherwise provided, directly or indirectly, goods, services, or technology to Iran or Syria which is likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of Iran or Syria, as well as anyone who materially assisted, sponsored, or provided financial, material or technological support of such activities.

13.6.4. Restated and Revised Iranian Transactions and Sanctions Regulations ("ITSR"). In an effort which was clearly underway for some time, on October 22, 2012, OFAC issued restated and revised Iranian Transactions Regulations which will now be called the Iranian Transactions and Sanctions Regulations ("ITSR"). The new regulations are an effort to update and clarify all the Executive Orders and which have been issued since 1987 into a new comprehensive set of regulations. A very commendable effort by OFAC, except for the fact that they do not include the provisions of the October 9, 2012 Executive Order implementing the ITRSHRA. The ITSR include new requirements for specific licenses and also issues new general licenses, primarily in the food, medicine and medical devices areas.

13.6.5. Most Sanctions Against Burma Lifted. Following the recent political reforms and successful democratic elections in Burma/Myanmar, OFAC issued new general licenses, General Licenses 16-19, described further below, lifting most of the sanctions against

Burma. The European Union and Canada suspended their respective sanctions against Burma back in April of 2012, except for the arms embargo and sanctions targeting certain individuals and entities. Senior U.S. government officials hinted that the United States would soon follow suit, but the complexities of doing so and pushback from Congress and human rights organizations delayed implementation. However, on July 11, 2012, OFAC finally issued the much anticipated General Licenses 16 and 17, which were later followed by General Licenses 18 and 19. The changes relaxed the country-wide prohibitions of the Burmese Sanctions Regulations, but generally maintained, and actually added to, the targeted blocking orders that form a major part of the U.S. sanctions.

Unusually in the context of a "relaxation" of sanctions, the President issued a new Executive Order on July 11, 2012, the sixth Executive Order with regard to Burma, and the fourth implementing assets blocking, complementing the mandatory assets blocking provisions of the 2008 JADE Act. *See* Executive Order 13619, RLINK"http://www.gpo.gov/fdsys/pkg/FR-2012-07-13/pdf/2012-17264.pdf"\l"page=1"77 *Fed. Reg.* 41243 (July 13, 2012). The new Executive Order blocks the property of persons designated as having threatened the peace, security, or stability of Burma; or to have been responsible for or complicit in human rights abuses; or to have been involved in proliferation-related activity involving North Korea. The Burmese Directorate of Defense Industries is so far the only party designated under the July 11, 2012 Executive Order.

One of the key OFAC concepts reinforced by the June 11, 2012 Executive Order is the notion that entities in which an SDN owns 50 percent or more, or an otherwise controlling interest, are subject to the same restrictions as a party who is actually designated. So, it continues to be important to screen the ownership of entities with whom U.S. persons do business in Burma.

At the same time, OFAC issued two general licenses under the existing Burmese Sanctions Regulations. General License 16 authorized the export of financial services to Burma, except to those persons designated under Executive Order 13448, Executive Order 13464, or the June 11, 2012 Executive Order. This General License did not authorize dealings with persons designated under the JADE Act, although this is a moot point, because all parties designated under the JADE Act are doubly designated under EO 13448 or 13464. Inwa Bank, which was not previously designated, was added to the SDN List pursuant to Executive Order 13464, so is not eligible to receive financial services under this general license.

General License 16 authorized the export of financial services to persons named under Executive Order 13310, which includes Myanma Foreign Trade Bank, Myanma Investment and Commercial Bank, and the Myanma Economic Bank. Thus, while the General License did not un-block those banks (e.g., a U.S. person could not open an account there), it permitted the indirect export of financial services to them. We use the term "indirect" because, despite these changes, there still could be no direct transactions between Executive Order 13310 SDN banks and the U.S. financial system after General License 16. That meant the SDN banks could be involved in otherwise authorized financial transactions involving Burma, but transfers had to be

 bflowe@bcr-dc.com

via a third country bank. Such funds, having come to rest in a third country bank, can then be transferred freely.

Subject to certain reporting requirements, General License 17 authorized new investments in Burma, except they could not involve an agreement with the Burmese Ministry of Defense, any state or non-state armed group, or any SDN blocked under Executive Order 13448, Executive Order 13464, or the June 11, 2012 Executive Order. This General License did not authorize dealings with persons designated under the JADE Act, although that is also a practical moot point because, again, all parties designated under the JADE Act are doubly designated under Executive Order 13448 or Executive Order 13464.

There are two State Department reporting requirements under General License 17. The first report essentially requires U.S. persons with aggregate investments in Burma exceeding $500,000 to submit a rather detailed report (annually by the first of April for the preceding year) describing the nature of the business in Burma, the names of the companies involved, the locations of the operations, and the approximate maximum number of both Burmese and non-Burmese employees in Burma. The report must also include a summary or copies of a number of enumerated company policies and procedures, such as due diligence, anti-corruption, social responsibility, and employment policies and procedures, among others. It must also include information on any arrangements with security service providers, property acquisition, certain payments made to the Burmese government, any meetings with military entities in Burma, and any steps taken to mitigate human rights, worker rights, and environmental risks. Two versions of the report must be submitted, a public and government-only report, with the public report including a bit less information than the government-only report.

The second report is only required for U.S. persons undertaking new investment pursuant to an agreement, or the exercise of rights under such an agreement, entered into with Myanma Oil and Gas Enterprise ("MOGE"). This report is much shorter than the one above, requiring only that the U.S. person notify the State Department within 60 days of the new investment.

Both of the reports may be submitted by email. Additional details on the reports, including where to submit them, are available at http://www.humanrights.gov/wp-content/uploads/2012/07/Burma-Responsible-Investment-Reporting-Reqs.pdf.

On September 19, 2012, OFAC announced that it took the additional step of removing the Burmese president and and speaker of the lower house from the SDN list, to personally reward them for taking "concrete steps to promote political reforms and human rights. . . ." Since taking office in early 2011, the Burmese president has supported a number of reform measures, including granting amnesty to many political prisoners, and maintaining a dialogue with Aung San Suu Kyi, the opposition party leader recently released from house arrest and elected to parliament. On the same day, Treasury's Financial Crimes Enforcement Network (FinCen) announced that it would be removing Patriot Act restrictions on two Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank. However, as both of these banks are defunct it was largely a symbolic measure.

 bflowe@bcr-dc.com

Next, OFAC issued General License 18, which authorized the importation of products of Burma. However, that General License was removed following issuance of Executive Order 13651 on August 7, 2013, prohibiting certain imports of Burmese jadeite and rubies. Executive Order 13651 repealed the provisions of Executive Order 13310 that implemented the broad Burmese Freedom and Democracy Act import ban on products of Burma, but maintained the ban on imports of Burmese jadeite, rubies, and jewelry containing the same, due to continuing labor and human rights concerns in the jadeite and ruby mining industries.

Finally, General License 19, issues February 22, 2013, went a step further than General License 16 and authorized almost all transactions, including opening and maintaining accounts, with four of Burma's major banks – Myanma Economic Bank, Myanma Investment and Commercial Bank, Asia Green Development Bank, and Ayeyarwady Bank. The General License did not authorize: (i) transactions involving blocked parties other than those banks; (ii) exportation of financial services, in connection with the provision of security services, directly or indirectly, to the Burmese Ministry of Defense, any armed group, or any entity in which any of the foregoing owns a 50 percent or greater interest; (iii) any "new investment," as defined in 31 C.F.R. 537.311, including with the four named banks; or (iv) the importation of Burmese jadeite or rubies, or jewelry containing the same. The General License also noted that the provisions of Section 311 of the Patriot Act no longer apply to the operation of correspondent accounts for the four named banks, or to transactions conducted through those accounts.

All told, the only sanctions now remaining against Burma are the orders blocking the property of specific individuals and entities, the arms embargo prohibiting the export of any defense articles or services to Burma and the ban on the importation of Burmese origin jadeite, rubies and jewelry containing the same. If this incremental cooperation continues, we would not be surprised to see additional individuals and entities removed from the SDN list in the future; we do not expect to see any quick changes regarding the arms embargo, however.

13.6.6. <u>Update On Sanctions Against Syria</u>. Sanctions against Syria remain in place and have not been further tightened (save for as described above), although OFAC has issued a few more of the general licenses that are common fixtures in the comprehensive OFAC sanctions regimes (i.e., Cuba, Iran, Sudan). They are summarized below, for your reference (but we of course advise carefully reviewing the licenses *and all of their conditions and limitations* prior to relying on any of them).

- **General License 7** – Winding Down Contracts Involving the Government of Syria; Divestiture of a U.S. Person's Investments or Winding Down of Contracts Involving Syria. Authorized certain transactions ordinarily incident and necessary to winding down contracts involving the Government of Syria (but only through November 25, 2011).
- **General License 8 –** Official Activities of International Organizations. Authorizing transactions for the conduct of the official business of the United Nations by employees, contractors or grantees thereof, provided that contractors or grantees provide a copy of their contract/grant in advance of U.S. persons engaging in or facilitating any such transactions.

 bflowe@bcr-dc.com

- **General License 9 –** Transactions Related to U.S. Persons Residing in Syria. Authorizing U.S. persons residing in Syria to pay their personal living expenses in Syria (including housing expenses, acquisition of goods and services for personal use, payment of taxes or fees to the Government of Syria, etc.) and to engage in other transactions ordinarily incident and necessary to their personal maintenance in Syria.
- **General License 10 –** Operation of Accounts. Authorizing the operation of an account in a U.S. financial institution for any unblocked individual in Syria, provided that any transactions processed are of a personal nature and not for use in support of or operating a business, and do not involve transfers directly or indirectly to Syria or for the benefit of individuals ordinarily resident in Syria (unless a noncommercial personal remittance).
- **General License 11A –** Authorizing Certain Services in Support of Nongovernmental Organizations' Activities in Syria. Authorizing NGOs to export/reexport services to Syria in support of not-for-profit humanitarian projects, democracy building or educational activities, non-commercial development projects directly benefiting the Syrian people, or activities to support the preservation and protection of cultural heritage sites in Syria. (General License 11A expanded upon and superseded its predecessor, General License 11.)
- **General License 12 – Third-Country Diplomatic Consular Funds Transfers.** Authorizing funds transfers for the operating expenses or other official business of third-country diplomatic or consular missions in Syria, provided the transfers are not by, to, or through the Government of Syria or any other blocked person.
- **General License 13 – Allowable Payments for Overflights of Syrian Airspace.** Authorizing payments to the Government of Syria in connection with the overflight of Syria or emergency landing in Syria, provided no payments are made by, to, or through any other blocked person.
- **General License 14 – Transactions Related to Telecommunications Authorized.** Authorizing all transactions with respect to the receipt and transmission of telecommunications involving Syria, provided no payment involves any debit to an account of the Government of Syria on the books of a U.S. financial institution or any transaction with a blocked person other than the Government of Syria, there is no provision of equipment or technology, and there is no provision of capacity on telecommunications transmission facilities to Syria.
- **General License 15 – Certain Transactions Related to Patents, Trademarks, and Copyrights Authorized.** Authorizing transactions related to the filing and prosecution of an application to obtain intellectual property ("IP") protection (i.e. patents, trademarks, copyrights), the receipt of IP protection, the renewal or maintenance of IP protection, the filing and prosecution of any opposition or infringement proceeding with respect to IP protection, or entry of a defense to any such proceeding.

Although referenced above, it bears repeating that most of these general licenses are subject to a number of conditions and limitations that should be carefully considered, with the assistance of counsel as necessary, prior to reliance on the license. We also note that the most recent round of sanctions against Syria have not yet been implemented in regulations, meaning that we do not yet have the benefit of any refinement, clarification or interpretive guidance that may (or may not) be provided in the regulations once they are published.

 bflowe@bcr-dc.com

13.6.7. Update on Sanctions Against Sudan.

13.6.7.1. OFAC Liberalizes Sudanese Sanctions Regulations in Connection With the Republic of South Sudan. While OFAC long ago amended its rules to exclude the areas now comprising the new nation of South Sudan from OFAC sanctions, many transactions with South Sudan involve ancillary activities via Sudan (i.e., northern Sudan) that still required an OFAC license, such as any oil and gas related transactions, transportation through Sudan to South Sudan (which has no ports or major airports), and many banking activities.

On December 8, 2011, OFAC revised its Sudanese Sanctions Regulations ("SSR") (31 C.F.R. Part 538) to eliminate most OFAC licensing requirements on such ancillary activities. 76 Fed. Reg. 76617 (Dec. 8, 2011). In its final rule, OFAC made two main changes: (1) added a new SSR § 538.536 to authorize virtually all activities and transactions relating to the petroleum and petroleum industries in South Sudan, and (2) added a new SSR § 538.537 to authorize the transit or transshipment of goods, technology, and services through Sudan to or from South Sudan. Among other things, new SSR § 538.536 authorizes the transshipment of goods, technology, and services relating to petroleum industries to or from South Sudan through Sudan, but does not authorize the refining in Sudan of petroleum from South Sudan. Financial transactions ordinarily incident to the activities authorized by SSR §§ 538.536 and Part 537 are also authorized, subject to certain limitations.

While the revised SSR greatly simplifies compliance concerning transactions with South Sudan, it still would be easy to violate the SSR inadvertently while doing business with South Sudan. So, be careful to ensure that OFAC and BIS licenses are not needed or that you obtain licenses that are required.

Exports/reexports to South Sudan that are subject to U.S. jurisdiction continue to be required to comply with other applicable U.S. export controls, such as the EAR and the ITAR. Also, Sudan (northern Sudan) continues to be subject to a U.S. embargo, which is administered mainly by OFAC, BIS, and DDTC.

13.6.7.2 Sudan General License 1 Issued, Authorizing Certain Academic and Professional Exchanges. On April 15, 2013, OFAC issued General License 1 authorizing certain academic and professional exchange activities between the United States and Sudan, which are otherwise prohibited by the Sudanese Sanctions Regulations (31 C.F.R. Part 538), subject to the conditions set forth in the general license. General License 1 allows accredited degree-granting colleges and universities located in or organized under the laws of the United States (or any jurisdiction within the United States) to enter into agreements to establish and operate academic exchange programs with similar academic institutions in Sudan, including such institutions that fall within the definition of the term Government of Sudan in §538.305 of the Sudanese Sanctions Regulations. Students attending U.S. colleges and universities are authorized to participate in academic programs at colleges and universities in Sudan for academic credit, and U.S. persons are authorized to teach the humanities, social and

environmental sciences, agriculture, public works, public health, law, and business at colleges and universities located in Sudan.

General License 1 also authorizes U.S. persons to administer professional certificate and university entrance examinations (such as the TOEFL, SAT, ACT, GRE, LSAT, and MCAT), and to conduct professional training seminars in the aforementioned subject areas on a not-for-profit basis, in each case for the benefit of persons in Sudan. In addition, General License 1 permits certain U.S. persons to conduct research in Sudan for noncommercial studies.

General License 1 also authorizes U.S. financial institutions to process funds transfers from persons located in Sudan (including the Government of Sudan) to enable students to participate in academic exchange programs, so long as any transaction between a U.S. financial institution and the Government of Sudan is first transited through an intermediary financial institution. General License 1 also permits U.S. financial institutions to accept and process student loan payments from students located in Sudan.

Finally, subject to specified restrictions, General License 1 permits the release of certain technology and software to Sudanese students attending school in the United States, so long as the technology is designated EAR99, or constitutes educational information not subject to the EAR (as set forth in 15 CFR 734.9).

13.6.7. Sanctions Against Libya Relaxed. The sanctions against Libya, established in 2011 in response to the extreme measures taken by the former Government of Libya against the Libyan people, targeted primarily the Government of Libya and specific individuals, such as the late Colonel Muammar Qadhafi and his family members. Due to the United States' subsequent recognition of the rebel forces of the Transitional National Council ("TNC") of Libya as the legitimate governing authority in Libya, the sanctions have since been relaxed as to the "Government of Libya." Specifically, a few additional general licenses have been issued, as summarized below. As with the Syria general licenses, summarized above, we advise careful review of these general licenses, and any and all conditions and limitations thereto, before the licenses are employed.

- General License 6 – Authorizing all transactions involving the TNC, provided they do not involve any blocked persons (property and interests therein of Qadhafi, and members of his family and regime that were blocked remain blocked).
- General License 7A – Authorizing all transactions involving the Libyan National Oil Company, provided such transactions involve no blocked persons.
- General License 8A – Authorizing all transactions with the Government of Libya and the Central Bank of Libya, provided such transactions involve no blocked persons.
- General License 9 – Unblocking all funds and precious metals of the General National Maritime Transport Company, subject to certain reporting requirements.
- General License 10 – Unblocking the Arab Turkish Bank and North African International Bank, subject to certain reporting requirements.
- General License 11 – Unblocking the Government of Libya and Central Bank of Libya, but noting that all funds and precious metals of the Libyan Investment Authority remain blocked.

 bflowe@bcr-dc.com

These last few general licenses, subject to the conditions and limitations not fully articulated here, largely reversed many of the sanctions established in 2011. The remaining sanctions primarily target the Qadhafi family and certain members of the former Qadhafi regime.

Conclusion

I hope that this summary helps provide some insight into the arcane law of U.S. reexport controls. The complexities demonstrate why companies that do regular business with the United States are wise to establish programs to promote efficient compliance with these impediments to business and to minimize risks of violations.

Disclaimer: This paper contains general legal guidance on the matters discussed herein, but should not be construed as specific legal advice or a legal opinion on the application of this guidance to any specific facts or circumstances. Opinions contained herein are solely those of the author and do not necessarily reflect the opinions of other members of this firm. Please feel free to contact the author with specific questions. I appreciate very much the able assistance of my colleagues Michelle Turner Roberts, Wayne Rusch, Dan Fisher-Owens, John Ordway, Ray Gold, and Jason McClurg in preparing this version of this paper.

-#-

Attachments

Customer Export Compliance Checklist Reference Form
Know Your Customer Guidelines
Country Groups from EAR Part 740

 bflowe@bcr-dc.com

CUSTOMER EXPORT COMPLIANCE CHECKLIST REFERENCE FORM

A. Sales Representative to Complete (and provide to Export Compliance Administrator ("ECA")):

1. Diversion Risk Screen. Are any of the attached high risk of diversion elements present?
___ No. (Proceed to next item.)
___ Yes. (Flag to hold order and consult with ECA. Note how questions were resolved here. _____.)

***2. Sensitive Nuclear Screen.** Does Company have any information that the customer is involved in: design, development, fabrication, or testing of nuclear weapons or explosive devices; or design, construction, fabrication, or operation of facilities or components of facilities for chemical processing of irradiated special nuclear or source material, heavy water production, separation of isotopes of source and special nuclear material, or fabrication of nuclear reactor fuel containing plutonium, or unsafeguarded nuclear facilities? ___ No. (Proceed to next item.)
___ Yes. (Flag to hold orders and consult with ECA. Note how any questions were resolved here. _____.)

3. Missile Screening. Does Company have any information that the customer is involved in direct or indirect assistance in the design, fabrication, operation, or maintenance of rocket systems (including ballistic missile systems, space launch vehicles, and sounding rockets); or unmanned air vehicle systems (including cruise missile systems, target drones, remotely piloted vehicles, and reconnaissance drones)? ___ No. (Proceed to next item.)
___ Yes. (Flag to hold orders and consult with ECA. Note how any questions were resolved here. _____.)

4. Chemical and Biological Weapons Screening. Does Company have any information that the customer is involved in design, development, production, stockpiling or use of chemical or biological weapons?
___ No. (Proceed to next item.)
___ Yes. (Flag to hold orders and consult with ECA. Note how any questions were resolved here. _____.)

5. Embargoed Countries. Does Company have any information that the customer is located in or intends to ship Company products to Cuba, Iran, North Korea, Syria, Sudan, or any other country subject to a current U.S. embargo or unilateral export controls. ___ No. (Proceed to next item.)
___ Yes. (Flag to hold orders and consult with ECA. Note how any questions were resolved here. _____.)

***6. Military End-Users/End-Uses.** Does Company have any information that the customer is part of any military or will be putting Company products to military end-use (ONLY FOR CIV, or certain NLR microprocessors to D:1 countries, or certain ECCNs to China, or to Iraq other than for U.S. and coalition forces)?
___ No. (Proceed to next item.) ___ Yes. (Flag to hold orders and consult with ECA. Note how any questions were resolved here. _____.)

Sales Person Name/Date: _____ ECA Verify: _____

* Note: Those items indicated by an asterisk do not apply to shipments to the European Community, Australia, New Zealand, or Japan. (See Supplement 3 to EAR Part 744 for a specific list of exempt countries.)

B. Export Compliance Administrator to Complete:

1. Denial Lists Screening. Are any parties listed on any of the current Denial Lists? [Can be based on customer screens.]
___ No. (Proceed.)
___Yes. (Consult with _____ for resolution. Note how resolved _____)

2. Product Classification/Licensing. Using current Company Product Matrix, are all products eligible for export under NLR or a License Exception to the applicable destination?
__ No. (Hold orders and flag to apply for License or use existing one if applicable, logging shipment against available License limits. Note License No. _____ and proceed after License obtained.

 bflowe@bcr-dc.com

__ Yes. (Note NLR or License Exception Symbol and ECCN here and on shipping documents and proceed: _____.) **NB: If using LVS or TMP, create/add to log for customer to ensure limits of those License Exceptions not exceeded.**
Export Compliance Administrator Name/Date:_____

 bflowe@bcr-dc.com

BIS's "KNOW YOUR CUSTOMER" Guidance and Red Flags

Certain provisions in EAR Part 744 require an exporter to obtain a license if the exporter "knows" that any export otherwise eligible for license exception is for end-uses involving nuclear, chemical, or biological weapons, or related missile delivery systems, in named destinations listed in the regulations.

(a) BIS has issued the following guidance on how individuals and firms should act under this knowledge standard. This guidance does not change or revise the EAR.

(1) Decide whether there are "red flags". Take into account any abnormal circumstances in a transaction that, indicate that the export may be destined for an inappropriate end-use, end-user, or destination. Such circumstances are referred to as "red flags". Included among examples of red flags are orders for items that are inconsistent with the needs of the purchaser, a customer declining installation and testing when included in the sales price or when normally requested, or requests for equipment configurations which are incompatible with the stated destination (e.g., 120 volts in a country with 220 volts). Commerce has developed lists of such red flags that are not all-inclusive but are intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate the EAR.

(2) If there are "red flags", inquire. If there are no "red flags" in the information that comes to your firm, you should be able to proceed with a transaction in reliance on information you have received. That is, absent "red flags" (or an express requirement in the EAR), there is no affirmative duty upon exporters to inquire, verify, or otherwise "go behind" the customer's representations. However, when "red flags" are raised in information that comes to your firm, you have a duty to check out the suspicious circumstances and inquire about the end-use, end-user, or ultimate country of destination. The duty to check out "red flags" is not confined to the use of License Exceptions affected by the "know" or "reason to know" language in the EAR. Applicants for licenses are required by part 748 of the EAR to obtain documentary evidence concerning the transaction, and misrepresentation or concealment of material facts is prohibited, both in the licensing process and in all export control documents. You can rely upon representations from your customer and repeat them in the documents you file unless red flags oblige you to take verification steps.

(3) Do not self-blind. Do not cut off the flow of information that comes to your firm in the normal course of business. For example, do not instruct the sales force to tell potential customers to refrain from discussing the actual end-use, end-user, and ultimate country of destination for the product your firm is seeking to sell. Do not put on blinders that prevent the learning of relevant information. An affirmative policy of steps to avoid "bad" information would not insulate a company from liability, and it would usually be considered an aggravating factor in an enforcement proceeding.

(4) Employees need to know how to handle "red flags". Knowledge possessed by an employee of a company can be imputed to a firm so as to make it liable for a violation. This makes it important for firms to establish clear policies and effective compliance procedures to ensure that such knowledge about transactions can be evaluated by responsible senior officials. Failure to do so could be regarded as a form of self-blinding.

(5) Reevaluate all the information after the inquiry. The purpose of this inquiry and reevaluation is to determine whether the "red flags" can be explained or justified. If they can, you may proceed with the transaction. If the "red flags" cannot be explained or justified and you proceed, you run the risk of having had "knowledge" that would make your action a violation of the EAR.

(6) Refrain from the transaction or advise BIS and wait. If you continue to have reasons for concern after your inquiry, then you should either refrain from the transaction or submit all the relevant information to BIS in the form of an application for a license or in such other form as BIS may specify.

(b) Industry has an important role to play in preventing exports and reexports contrary to the national security and foreign policy interests of the United States. BIS will continue to work in partnership with industry to make this front line of defense effective, while minimizing the regulatory burden on exporters. If you have any question about whether you have encountered a "red flag", you may contact the Office of Export Enforcement at 1-800-424-2980 or the Office of Exporter Services at (202)482-4532.

 bflowe@bcr-dc.com

RED FLAGS

Possible indicators that an unlawful diversion might be planned by your customer include the following:

1. The customer or purchasing agent is reluctant to offer information about the end-use of a product.

2. The product's capabilities do not fit the buyer's line of business; for example, a small bakery places an order for several sophisticated lasers.

3. The product ordered is incompatible with the technical level of the country to which the product is being shipped. For example, semiconductor manufacturing equipment would be of little use in a country without an electronics industry.

4. The customer has little or no business background.

5. The customer is willing to pay cash for a very expensive item when the terms of the sale call for financing.

6. The customer is unfamiliar with the product's performance characteristics but still wants the product.

7. Routine installation, training or maintenance services are declined by the customer.

8. Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.

9. A freight forwarding firm is listed as the product's final destination.

10. The shipping route is abnormal for the product and destination.

11. Packaging is inconsistent with the stated method of shipment or destination.

12. When questioned, the buyer is evasive or unclear about whether the purchased product is for domestic use, export or reexport.

 bflowe@bcr-dc.com

For Country Groups, see
http://www.bis.doc.gov/index.php/forms-documents/doc_view/452-supplement-no-1-to-part-740-country-groups

 bflowe@bcr-dc.com